


D7.4 Report on High Level Event

Deliverable submitted in December 2014 (M36) in fulfilment of the requirements of the FP7 project, ETTIS – European security trends and threats in society

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 285593.

	ETTIS Coordinator: Peace Research Institute Oslo (PRIO)	PO Box 9229 Grønland NO-0134 Oslo, Norway	T: +47 22 54 77 00 F: +47 22 54 77 01	www.ettis-project.eu
---	---	--	--	--

Project Acronym	ETTIS
Project full title	European security trends and threats in society
Website	www.ettisproject.eu; www.ettis-project.eu
Grant Agreement #	285593
Funding Scheme	FP7-SEC-2011-1 (Collaborative Project)
Deliverable:	D7.4
Title:	Validation report
Due date:	31. December 2014
Actual submission date:	17. December 2014
Lead contractor for this deliverable:	Fraunhofer INT
Contact:	Sonja Grigoleit Sonja.grigoleit@int.fraunhofer.de
Dissemination Level:	PU

Contributors:

Sonja Grigoleit, Fraunhofer INT
Hans-Martin Pastuszka, Fraunhofer INT
E. Anders Eriksson, Swedish Defence Research Agency
Maria da Graça Carvalho, Cabinet of the Commissioner for Research and Innovation
Nikos Kastrinos, European Commission
Tjien-Khoen Liem, European Commission
Antje Bierwisch, Fraunhofer ISI
J. Peter Burgess, Peace Research Institute Oslo
Ida Haisma, The Hague Security Delta
Ian Brown, Oxford University's Cyber Security Centre
Matthias Weber, Austrian Institute of Technology
Monica Lagazio, Trilateral Research & Consulting

1	INTRODUCTION	4
2	AGENDA	5
3	MEETING AND NETWORKING	7
4	SPEECHES, PRESENTATIONS AND DISCUSSIONS	10
4.1	Presentation of E. Anders Eriksson	10
4.2	Session 1 “Foresight-based societal approach to security research”	11
4.2.1	Presentation of Nikos Kastrinos	11
4.2.2	Speech of Tjien-Khoen Liem	12
4.2.3	Presentation of Antje Bierwisch.....	13
4.3	Speech of J. Peter Burgess.....	14
4.4	Presentation of Ida Haisma	15
4.5	Session 2 “Security research and innovation – the need to manage the diversity of challenges”	16
4.5.1	Presentation of Ian Brown.....	16
4.5.2	Presentation of Matthias Weber	17
4.5.3	Panel discussion	18
4.6	Speech of Monica Lagazio.....	19
5	CONCLUSION	20
6	ANNEX	23
6.1	List of Participants.....	23
6.2	Presentation of E. Anders Eriksson	25
6.3	Letter of Maria da Graca Carvalho	35
6.4	Presentation of Nikos Kastrinos	37
6.5	Speech of Tjien-Khoen Liem.....	43
6.6	Presentation of Antje Bierwisch	49
6.7	Speech of J. Peter Burgess.....	57
6.8	Presentation of Ida Haisma	64
6.9	Presentation of Ian Brown	73
6.10	Presentation of Matthias Weber	79
6.11	Speech of Monica Lagacio.....	85

1 INTRODUCTION

After three years full of intensive discussions both within the ETTIS consortium as well as with many different stakeholders in our ETTIS workshops and three years of working for the right way

- of understanding security not simply in terms of external threats and appropriate responses,
- of dealing with security research and innovation which includes both technological as well as societal aspects of security,
- of a security research which is geared better towards societal challenges and needs,
- of a research and innovation policy and programming which supports a comprehensive conceptualisation of societal security,

ETTIS celebrated its final event at 20th of November 2014 in Brussels.

This High Level Event took place in the Representation of the State of North Rhine-Westphalia to the EU in Brussels and had the aim to both disseminate the results of the ETTIS project to a larger audience as well as to discuss the ETTIS findings and methodologies with a broad range of different stakeholders.

This report contains both a summary of the different speeches and presentations of the event as well as impressions from the panel and plenum discussions. In the annex of this report the PowerPoint slides and the full speeches of the speakers can be found.



2 AGENDA

SHAPING SOCIETAL SECURITY IN THE EUROPEAN UNION

- A High Level Event -

9:00 – 9:30 **Welcome**
with Coffee & Cookies

9:30 – 9:45	Introduction to ETTIS	E. Anders Eriksson FOI
9:45– 10:15	Key note <i>Expectations of the European Parliament on the uptake of long-term societal security needs and challenges by EU research</i>	Maria da Graça Carvalho¹ Bureau of European Policy Advisers, EC MEP (2009-2014)
10:15 – 10:30	Coffee Break	
10:30 – 12:15	Session I “Foresight-based societal approach to security research” Chaired by Ewa Dönitz, Fhg ISI	
	<ul style="list-style-type: none">• <i>Foresight in Horizon 2020 Strategic Programming</i>	Nikos Kastrinos DG RTD A/6 Science Policy, Foresight and Data
	<ul style="list-style-type: none">• <i>Current approach of DG ENTR in the R&D planning for the “Secure Societies” programme</i>	Tjien-Khoen Liem DG ENTR G/4 Policy and Research in Security
	<ul style="list-style-type: none">• <i>Civil Security Research – future challenges and methodological outlook</i>• 	Antje Bierwisch Fraunhofer ISI
12:15 – 13:30	Lunch at “Beethoven”	
13:30 – 14:15	<i>From technological potential to societal planning: The ETTIS approach to security foresighting</i>	J. Peter Burgess ETTIS Coordinator
14:15 – 14:45	<i>Drafting of a National Security Innovation Agenda - how such an Agenda does justice to different societal security needs</i>	Ida Haisma Director, The Hague Security Delta

¹ Unfortunately Ms da Graça Carvalho had to cancel her speech at short notice due to another important assignment. She was so kind to send a letter summarising her key points, which is printed in Annex 6.3.

14:45 – 15:00	Coffee Break	
15:00 – 16:45	Session II “Security research and innovation – the need to manage the diversity of challenges” Chaired by E. Anders Eriksson, FOI	
	<ul style="list-style-type: none"> • Cybersecurity capability maturity model 	Ian Brown Oxford University's Cyber Security Centre
	<ul style="list-style-type: none"> • Mission-oriented RTI policy & programmes 	Matthias Weber AIT
16:45 – 17:00	Synthesis and closing	Monica Lagazio Trilateral
17:00 – 18:00	Informal Meeting at “Beethoven”	



3 MEETING AND NETWORKING

Thanks to the engaged and active participants of the High Level Event the day was filled with discussions about and around societal security, foresight, research and innovation (R&I) programming, mission-oriented innovation and many more aspects which are summarized in the exemplary questions below:²



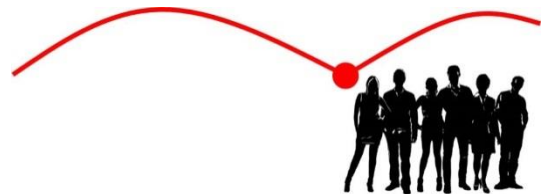
How can we deal with uncertainties?



How can we make sure that foresight is truly incorporated in policy making and strategic research and development (R&D) programming?



How can we implement the concept of “societal security” and societal needs into policy making and strategic R&D programming?



² The assignment of the questions to the pictures is purely accidental.



Is there a gap between what society needs and what industry can provide in terms of “security”?

What role does the private sector play in terms of societal security and what should it be?



How can the industrial base be more effective and efficient in terms of serving societal needs?

How to increase awareness and acceptance of participatory foresight approaches on the side of policy makers?



How do we plan for the future?



How can we deal with challenge-oriented research and innovation?

“80 percent of success is showing up”
Woody Allen



When is foresight useful? – When is it a luxury? - When is it not needed?

4 SPEECHES, PRESENTATIONS AND DISCUSSIONS

4.1 PRESENTATION OF E. ANDERS ERIKSSON

Currently Anders is Research Director (Systems Analysis) at the Swedish Defence Research Agency (FOI). Anders' main professional interests are how organisations should handle uncertainty, and in particular how they should harness foresight and innovation for this task.



In his comprehensive presentation Anders gave an overview of the results and achievements of the ETTIS project. He described the basis of our work – like the definition of the dimensions and sources of security – as well as our efforts to advance in the area of detecting future threats with different methods. He further introduced the audience into the context and domain scenarios developed by the ETTIS consortium. On the basis of our work in the three selected domains (nuclear, environment and cyber), the presentation described how the ETTIS consortium developed the four case studies – cyber defence systems, cyber civic resilience, climate and migration as well as professional security services.

Anders further explained the meta-model of innovation in security developed by ETTIS that covers a variety of potential constellations of security R&I systems. In this model the time frame available for R&I activities and the balance between social and technological features of innovation are the key dimensions for distinguishing the four archetypes of innovation models that cover the spectrum of security R&I systems:

- The modified industrial innovation model (which basically represents the current innovation model underlying EU security research),
- The fast and open innovation model,
- The social innovation model,
- The commons-oriented innovation model.

Lastly Anders introduced the proposed ETTIS governance framework for R&I, and for R&I programming and priority-setting in particular. Building on the requirements of the different innovation models in security, ETTIS proposes an adaptive process model of R&I programming, which would allow for a better reflection on and integration of societal security challenges and options in R&I programming. It builds on a re-interpretation and further development of the established, “standard” four phases of a programming cycle towards an adaptive four-phase-model. The adaptivity of this model would be ensured through continuous, bi-directional interaction and iteration between neighbouring phases, and complemented by a dedicated research basis placed in the centre of the process model, to support and ensure the scientific understanding of security challenges and options.

The PowerPoint presentation can be found in section 6.2.



4.2 SESSION 1 “FORESIGHT-BASED SOCIETAL APPROACH TO SECURITY RESEARCH”

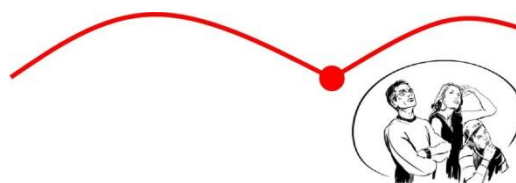
4.2.1 Presentation of Nikos Kastrinos

Nikos is a policy officer of the European Commission. He works in DG RTD, Unit A.6 – Science policy, foresight and data, and his responsibility is to ensure that foresight becomes a core part of the strategic approach that is needed for Horizon 2020.



Nikos gave an informative and interesting presentation about the use of foresight in strategic programming of Horizon 2020. After a historic overview of the application of foresight methods in various EU bodies, he described the current situation of foresight in EU institutions and processes. The focus of his presentation was on the use of foresight in strategic programming of Horizon 2020 itself and on the model of the European Forum on Forward Looking Activities (EFFLA). He further shared his experience with foresight in Horizon 2020 – about the advantages of using foresight, the necessary inputs and stakeholders of the foresight process as well as the plans and timeframes in the near future of the Horizon 2020 package. He concluded his presentation with a lessons-learned from the use of foresight in Horizon 2020 so far and the necessary conditions to get the most of foresight for R&D programming: according to him, the successful uptake of foresight intelligence requires a forward-looking culture of policy makers, a conducive anticipatory governance structure and good planning of foresight activities to match the policy calendars.

The PowerPoint presentation can be found in section 6.4.



4.2.2 Speech of Tjien-Khoen Liem

Khoen is principal scientific officer at the European Commission, DG ENTR G4 Policy and Research in Security (the Unit is becoming part of DG HOME right now). He was also a main driver among the first people setting-up Community Security Research in FP7.



Khoen gave in his clear and catchy speech an overview of the history of security research in the EU starting shortly after 9/11 in 2001. He underlined that the EU has to stop the reactive way of dealing with security (just providing “patches” to insecurity breaches). He said that we need to understand the underlying issues and that we also need to strengthen the resilience of the society. He further embedded the history of security research in the development of the European Union itself – starting from the Maastricht Treaty, and the Treaty of Amsterdam to the Lisbon Treaty.

He described the point of view of the new Juncker Commission regarding external actions, especially the project “a stronger global actor”, which lies in the responsibility of the new High Representative of the Union for Foreign Affairs and Security Policy, Ms Mogherini. Khoen pointed out that Europe has to take over a greater role in ensuring international peace and security and that it therefore has to ensure that it has the capabilities at its disposal which are required to meet the respective needs. In this context he underlined the importance of an integrated and competitive industrial base in the EU.

A further topic of his speech was dual-use research. He said that the increasingly dual character of technologies calls for a comprehensive approach in R&D. The “Secure Societies” Part of Horizon 2020 has parts that are already relevant for the Common Security and Defence Policy (CSDP) of the European Union – although the activities will maintain its strict civilian focus. The announced CSDP-Preparatory Action and the possible subsequent, future full research programme on CSDP resulting therefrom will be complementary.

The full speech can be found in section 6.5.



4.2.3 Presentation of Antje Bierwisch

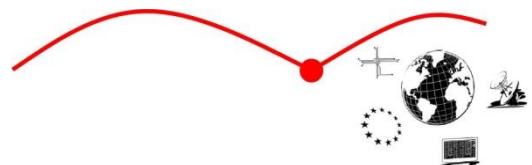
Since 2007 Antje Bierwisch has been working as a research project manager at the Competence Center Foresight at the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe. The focus of her research lies in the application and development of current methods of future research for national and international clients from industry, politics and science.



Antje started her well founded presentation by showing that civil security as treated in Horizon 2020 and the German national security programme are a paramount example for a mission oriented policy approach. She went on to describe the current challenges in foresight projects when dealing with innovation in civil security: the complexity of technology, the heterogeneity of stakeholders and the widening geographical scope. As another challenge she mentioned the aim to penetrate security research with ethical, legal, societal and political aspects as well as the aim of a cohesive society. This challenge leads to the concept of “Responsible Research and Innovation” (RRI). RRI is seen as a key capability to deal with societal challenges in the future.

In the second part of her presentation she elaborated on different foresight methods, which differ in the type of stakeholder involvement, time horizon, penetration depth, specialisation, etc. As an example she mentioned the EU project ETCETERA (Evaluation of critical and emerging technologies for the elaboration of a security research agenda) as well as the German national security research project SIRA (Security in public space).

The PowerPoint presentation can be found in section 6.6.



4.3 SPEECH OF J. PETER BURGESS

Peter is currently Research Professor at Peace Research Institute Oslo (PRIO) and Senior Researcher at the Institute for European Studies of the Vrije Universiteit Brussels. His research and writing concern the meeting place between science, culture and politics in particular in Europe, focusing most recently on the theory and ethics of security and insecurity.



In the opening of his profound speech Peter whisks the audience away to the world of the essayist, scholar and statistician N. N. Taleb and his influential book “The Black Swan”. A black swan is an outlier, an event that lies beyond the realm of normal expectations. These extreme events have a huge impact, especially due to the fact that they are unexpected. Nevertheless, people tend to find cogent explanations for these events retrospectively. The particularity of these future “black swan” events is that they are not known in the present. Black swans have this extreme impact due to two reasons – the event itself (e.g. the attacks of 9/11) and the unpredictability of these events and the insight about the meaning of our ignorance.

According to Taleb the application of risk management methods in social science or finance has its limits, due to the fact that what we do not know has far greater historical consequences than what we do know. If the risk of 9/11 had been reasonably conceivable on September 10, it would not have happened.

These observations have also implications for ETTIS which aim it is to identify future security threats so that we can prepare for them. The complexity of this task can be summarised in terms of three challenges: (1) We don’t know what will happen in the future, (2) We don’t know what security needs we will have in the future; (3) We don’t know what our capacities will be in the future.

Most approaches to plan for the future focus on capabilities. They try to understand what our future capabilities are, then to steer those capabilities so that we are best equipped to meet our needs. But in the framework of these fact-based approaches, we are dependent upon the facts about the future being correct. This dependency brings with it its own security risk.

The ETTIS project has sought to contribute an alternative to fact-dependent futurology, more oriented toward society. Peter concludes his speech by giving 10 ideas stemming from the output of ETTIS, e.g. the recommendation that research and innovation should start with an analysis of society - of how people live and that it should not only account for technological innovation but also for social innovation.

The full speech can be found in section 6.7.



4.4 PRESENTATION OF IDA HAISMA

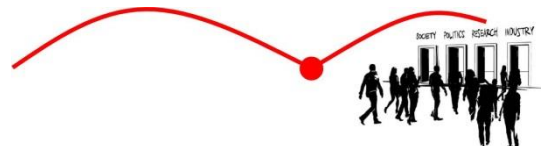
In 2014 Ida has taken up the position of Operational Director at The Hague Security Delta (HSD). At HSD Ida directs the programmes and projects. In addition, she is responsible for further development of the organisation and for the cooperation with the partners of HSD. Before her job at HSD, Ida was Director of Innovation for Safety and Security Research at TNO.



In her lively and enthusiastic presentation Ida introduced the audience to the Hague Security Delta (HSD), the largest security cluster in Europe which was opened in February 2014 with the aim to enhance security and stimulate economic development in the area of The Hague. In this Dutch cluster, companies, governments, and knowledge institutions work together on innovations and knowledge in the field of cyber security, national and urban security, protection of critical infrastructure, and forensics.

At the ETTIS event Ida presented the Dutch national innovation agenda for security as an example for an integrated approach to security. The agenda was requested by the Dutch Ministry of Security and Justice and developed by HSD, with the purpose to bring together demand, supply and knowledge to create societal/social and economic value. The agenda itself contains chapters about comprehensive security, innovation with regard to social and societal security, critical infrastructure, netcentric working/ networked environments, surveillance and unmanned systems as well as process innovation within and between professional organisations.

The PowerPoint presentation can be found in section 6.8.



4.5 SESSION 2 “SECURITY RESEARCH AND INNOVATION – THE NEED TO MANAGE THE DIVERSITY OF CHALLENGES”

4.5.1 Presentation of Ian Brown

Ian is Associate Director of Oxford University's Cyber Security Centre, and Professor of Information Security and Privacy at the OII. His research is focused on surveillance, privacy-enhancing technologies, and Internet regulation.



Ian did very well in breathing life into the more generic ideas discussed so far and presenting an example from the area of cyber security. Firstly, Ian introduced the Global Centre for Cyber Security Capacity Building, which aim it is to understand how to deliver effective cyber security both within the UK and internationally. The focus of his speech lay on the current development of a Capability Maturity Model (CMM). To introduce this topic he explained the five complementary dimensions of capacity the team will work with: (1) devising national cyber policy and cyber defence, (2) encouraging responsible cyber culture within society, (3) building cyber skills into the workforce and leadership, (4) creating effective legal and regulatory frameworks and (5) controlling risks through technology and processes. He gave an overview of the actual situation of the project and how the different maturity levels show the progress in each of the five dimensions.

In the second part of his speech he reported about a new model of PhD/DPhil at the Centre of Doctoral Training in Cyber Security. Remarkably these research projects will be undertaken in a wide variety of academic Departments and disciplines. Thus, apart from cyber security itself the courses will also include lectures about ethics, international relations and cultural norms or security policy.

The PowerPoint presentation can be found in section 6.9.



4.5.2 Presentation of Matthias Weber

Matthias is Head of the Research, Technology and Innovation Policy Unit at the AIT Innovation Systems Department. His current research interests include the impact of foresight on policy-making, the integration of innovation in sectoral and cross-cutting policies, and the governance of R&D collaboration networks.



Matthias gave the audience a clear and precise introduction into one of the key findings of the ETTIS project – how to develop mission-oriented RTI (research, technology and innovation) policy and programmes in the security field. He started his presentation by explaining the need for a new approach to security RTI programming. He reasoned that the current approach is mainly technology oriented and inspired by an industrial innovation model. Thus, in a new approach - beyond a threat-response model - the new mission-oriented R&I policy of Horizon 2020 (“Societal Challenges”) as well as the aspects of a societal security (the societal needs) have to be taken into account.

Matthias then went on by explaining the ETTIS meta-model comprising four archetypes of security innovation that cover a variety of potential constellations of security R&I systems. Both the time frame and the balance between social and technological features of innovation are key dimensions for distinguishing between these four archetypes.

The focus of his speech lay on the introduction of an adaptive process model of R&I programming. The model ETTIS proposes is a re-interpretation of the established four phases of a programming cycle, but is of a highly flexible and adaptive nature that can also draw on other than centralised approaches to prioritisation and implementation. This means e.g. that scientific research for better understanding security challenges and options need to be established and connected with the R&I programming.

He further mentioned the ten operational requirements for R&I programming and priority-setting in security, such as the consideration of both social and technological innovation, or the need for a flexible and adaptive model of R&I programming. Foresight processes can play an important role and can be used to support the entire programming cycle, both by informing the different stages of levels of R&I programming and by involving users and stakeholders throughout all phases of programming.

The PowerPoint presentation can be found in section 6.10.



4.5.3 Panel discussion

Chair:

- E. Anders Eriksson
Swedish Defence Research Agency (FOI)



Panellists:

- Matthias Weber, Austrian Institute of Technology
- Ian Brown, Oxford University's Cyber Security Centre
- Ida Haisma, The Hague Security Delta
- Nikos Kastrinos, European Commission
- Tjien-Khoen Liem, European Commission

Inspired by the two introductory presentations of Matthias Weber and Ian Brown the four panellists were engaged in lively discussions about e.g. research and innovation programming, innovation models, the role of industry, the use of foresight and societal security in general. A summary of the discussion is included in the synopsis in chapter 5.

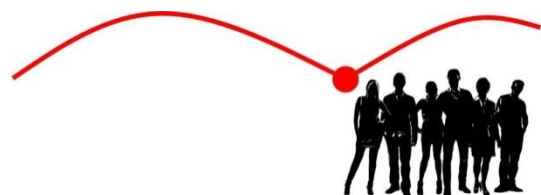
4.6 SPEECH OF MONICA LAGAZIO

Monica Lagazio is an associate partner at Trilateral Research & Consulting. Her work focuses on security, risk analysis, innovation, data strategy, and policy formulation.



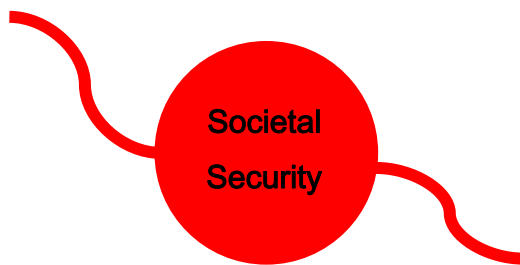
Towards the end of the High Level Event Monica gave a short and comprehensive synthesis of ETTIS to review the initial aims of the project and link them to our results. She started with the recapitulation of the key topics and questions the ETTIS consortium had to deal with when starting the project three years ago, like “What is the meaning of security and needs to be secured?” or “How can we prioritise in a complex security landscape?”. She then concisely connected these questions to the achievements of ETTIS like our concept of societal security, the tools and methods used to identify threats, needs and solutions and our adaptive four phase model of R&I programming. She closes her speech by giving an outlook of the further dissemination of the ETTIS research works through various channels.

The PowerPoint presentation can be found in section 6.11.



5 CONCLUSION

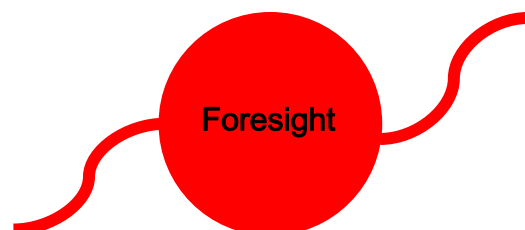
It was a pleasure to spend the day with all the engaged and enthusiastic participants of the ETTIS final event, who are all working on the big picture to chance European security research and innovation to be more oriented towards society – to include more social aspects. While it is impossible to include in this report all ideas and bits and pieces of the discussions, we certainly want to present some of the recurring topics of the day as they are summarised in the following synopsis:



There was a general consensus about the necessity to better include aspects of societal security into future research and innovation activities of the European Union. The EU should go beyond purely reactive approaches by providing “patches” to insecurity breaches and follow the idea of a comprehensive security instead. One reason for that was seen in the simple fact that it is economically and socially not affordable to secure the society with “patches” against all possible security threats. Therefore it was seen as necessary to better balance the security research agenda towards technical and social aspects.

It was also mentioned that there is a need to add European value. The national research agenda in Europe are very diverse – some nations don’t have a security research agenda at all, so we have to make sure that the European security research goes beyond those national efforts. It was further mentioned that the European Parliament should be more involved in this topic and that it should push the thinking in the direction of a comprehensive societal security.

Discussions about foresight were also very prominent throughout the day. It started from questions like “Who is doing foresight?” and the need to find a good combination of people with different backgrounds (scientists and policy makers) when being engaged in foresight processes. It was also asked how we could make sure that foresight is appropriately incorporated in relevant projects, and that its findings are heard by decision makers. Several participants stressed the importance of the



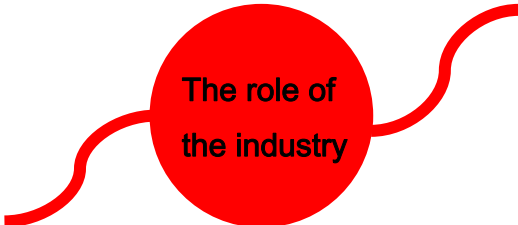
inclusion of foresight in security research. It was commented that foresight goes beyond providing “new information” (which are not new anymore once they are presented). To do foresight it was stated that we have to engage trustable and smart persons. It was also said that we have to decide when foresight brings an added value, when it is a luxury and when it is not needed.



Methods

It was mentioned that many research projects are strong in terms of methodology, but that they need to say more explicitly how to improve policy. The difficult question we have to solve is how to best spend the money for the right projects.

Somewhat different views were observed regarding the role of the industry in security research. Some of the participants were worried that there might be a gap between the aim of a comprehensive societal security on the one side and the need to strengthen the industrial basis of Europe on the other side. Others didn't see such a gap – they stated that the industry delivers what we need. It was said that the industry is crucial for us; it creates jobs and good lives for the people and thereby contributes in particular to our secure environment.



The role of the industry

While some participants stressed the fact that there is a need to “educate” industry about societal security aspects and needs, others opposed this view, stating that industry is well aware of these needs as it is an integral part of our society.

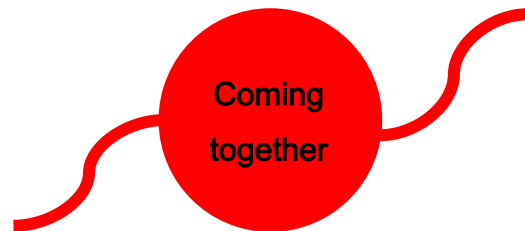


Societal challenges

One of the current societal challenges which were discussed during the ETTIS event are e.g. the problem of the aging Europe while globally there are more young people than ever before. According to the UNFPA 2014 State of World Population report many countries have the highest proportion of

young people in history, which in the end could lead to the movement of people. It was mentioned as an example to show, that Europe has to think more globally, and that this needs to be better reflected in EU R&I programming as well.

A not new but important insight of this event was also the need for different stakeholders (scientists, policy makers, industry representatives, etc.) to meet and speak to each other. To tackle the current and future challenges of societal security it is of outmost importance to engage people with different backgrounds and from different communities – to make them come together, to build bridges, to help to better understand each other and to discuss security issues from all relevant perspectives.



What remains to be done is to spread the findings of ETTIS to the broader stakeholder community in security. The ETTIS consortium is active in doing so by uploading all our deliverables, presentations, policy briefs, newsletters and scientific articles to our homepage <http://ettis-project.eu/> . Shortly there will also be a video available containing the main messages of ETTIS.



6 ANNEX

6.1 LIST OF PARTICIPANTS

Last Name	First Name	Organisation
Ackx	Vicky	Peace Research Institute Oslo
Adler	Christine	LMU München
Barbero	Fernando	Indra
Bierwisch	Antje	Fraunhofer ISI
Braun	Anette	VDI Technologiezentrum GmbH
Brown	Ian	Oxford University's Cyber Security Centre
Burgess	J. Peter	Peace Research Institute Oslo
Canet	Géraud	Atomic Energy and Alternative Energies Commission
Deering	Daniel	Centre for Irish and European Security
Dönitz	Ewa	Fraunhofer ISI
Eriksson	Anders	Swedish Defence Research Agency
Grigoleit	Sonja	Fraunhofer INT
Haisma	Ida	The Hague Security Delta
Huber	Katrin	European Parliament
Kastrinos	Nikos	European Commission
Jans	Karlijn	Netherlands Organisation for Applied Scientific Research (TNO)
Klerx	Joachim	Austrian Institute of Technology
Kliuyeva	Katsiaryna	European Organisation for Security
Lagazio	Monica	Trilateral Research & Consulting
Liem	Khoen	European Commission

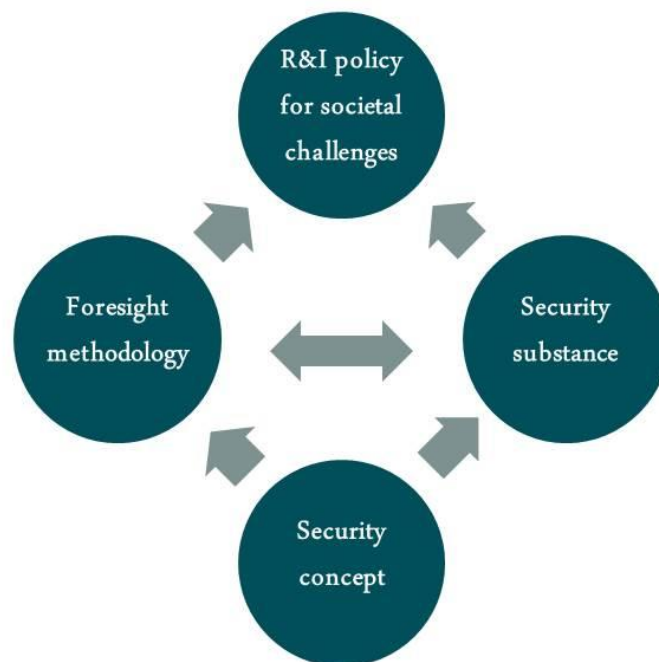
Martinez	Marina	Spanish Office for Science and Technology
McCarthy	Sadhbh	Centre for Irish and European Security
Meredith	Dora	Innovate UK
Morthens	Soley	NordForsk
Pastuszka	Hans-Martin	Fraunhofer INT
Bellanova	Rocco	Peace Research Institute Oslo
Shala	Erduana	Fraunhofer ISI
Suchier	Jean-Marc	Morpho
Sweijs	Tim	Hague Centre for Strategic Studies
Tigner	Brooks	Security Europe
Trcek	Denis	University of Ljubljana
Weber	Matthias	Austrian Institute of Technology
Weiland	Sigrid	European Commission
Wepner	Beatrix	Austrian Institute of Technology
Wetzling	Thorsten	Brandenburg Institute for Society and Security
Zupka	Dusan	UNDP Crisis and Disaster Risk Management Advisor
Häfner	Claudia	Helmholtz Gemeinschaft
Mitchener-Nissen	Timothy	Trilateral Research Consulting
Jones	Chris	Statewatch



Shaping societal security in the European Union

Project overview

Dr E. Anders Eriksson, FOI
20 November 2014
Brussels

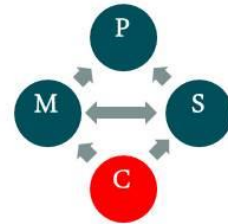


Dimensions of security

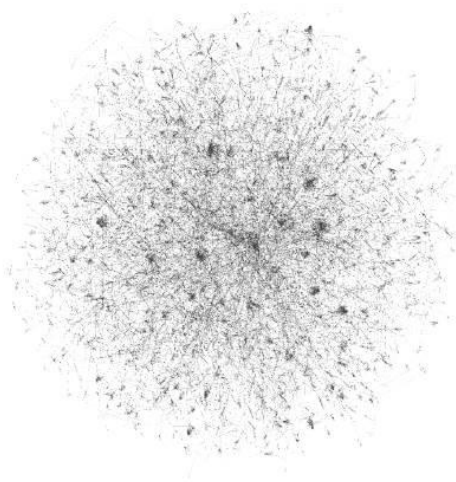
- Territorial security
- Economic security
- Technology and information security
- Physical/health security
- Environmental security
- Social and political stability
- International law

Sources of security

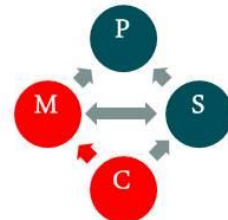
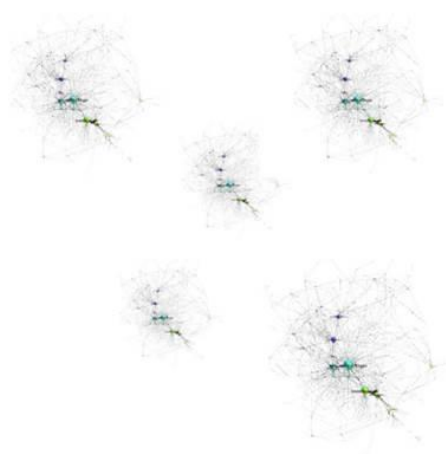
- Identity and social context
- Prevention
- Resilience
- Physical and social security technologies
- Education and assistance
- Language and communication
- Integrity and trust
- Ownership and incentive structures
- Coercion, compellence and deterrence



Typical high integrated epistemic community



The “future threats” network(s)

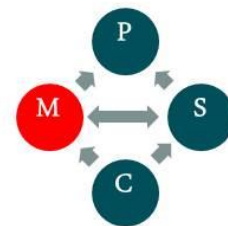
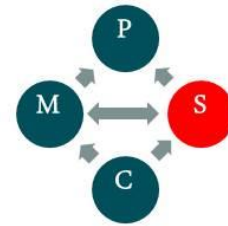


Three domains

**Cyber
infrastructure**

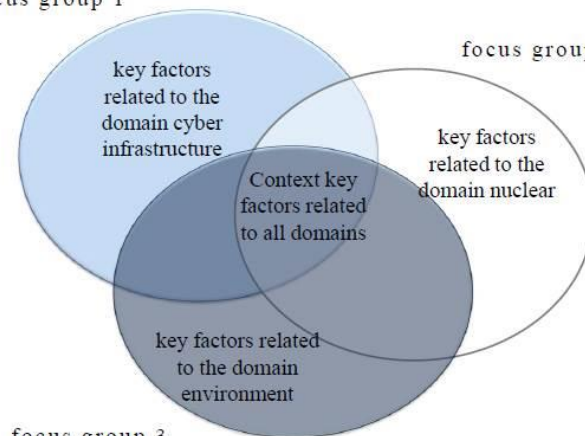
Environment

Nuclear material



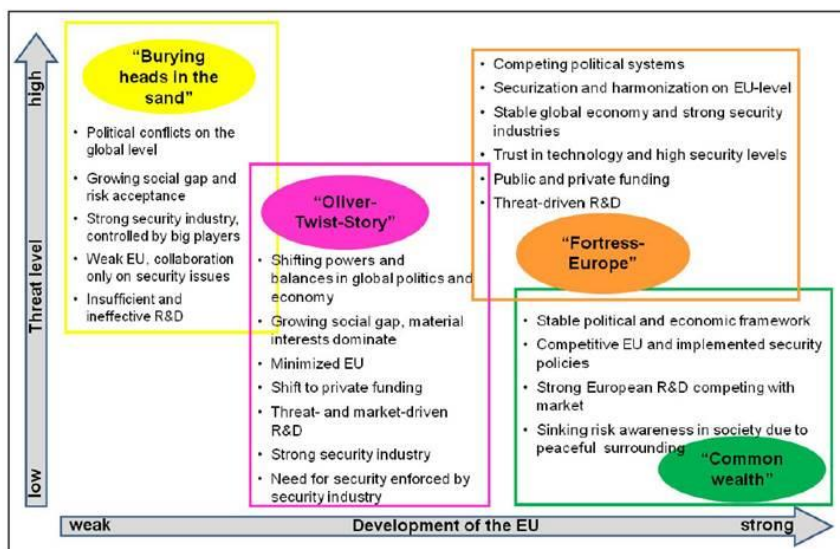
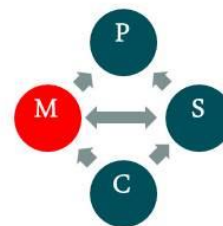
focus group 1

focus group 2

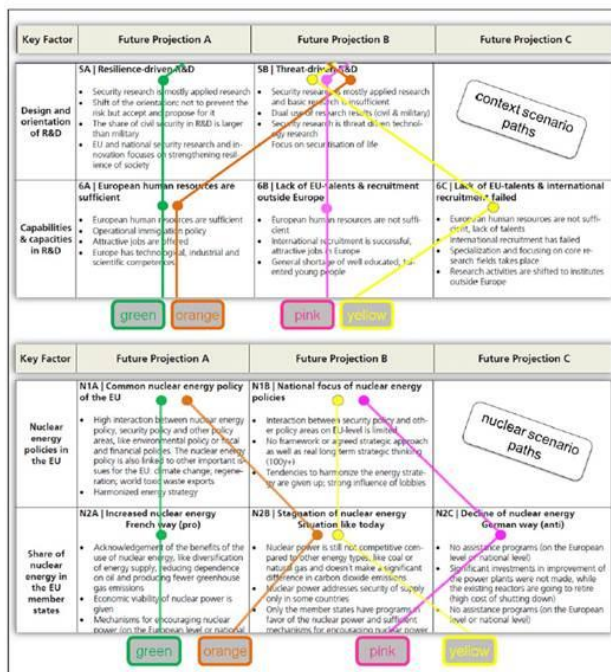
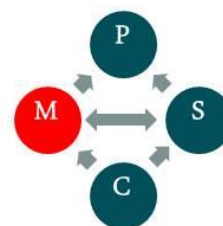


focus group 3

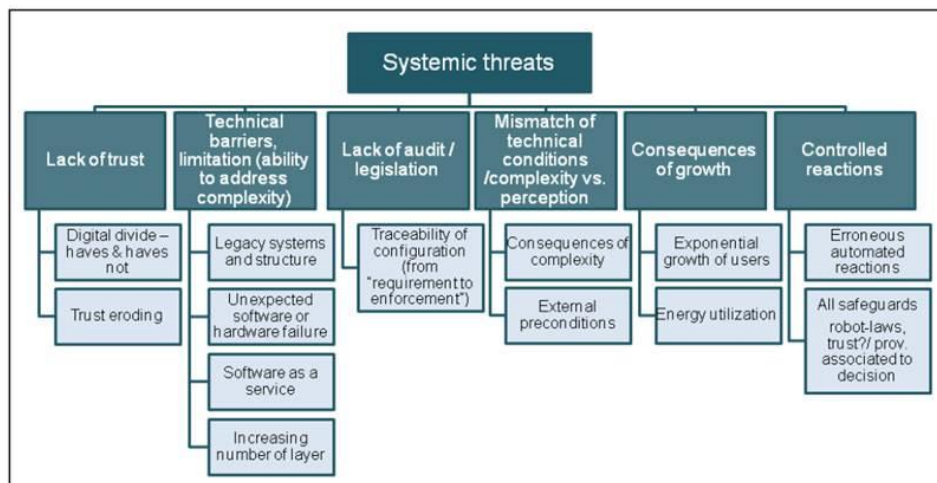
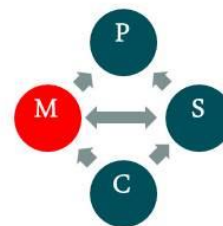
The four context scenarios for two key characteristics



Nuclear domain scenario (detail)

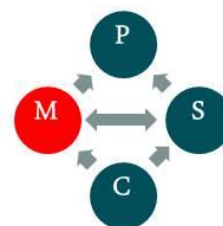
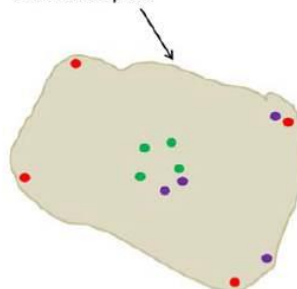


Threat scenario analysis

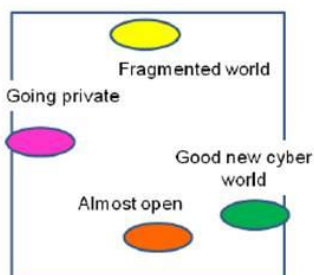


Requisite diversity of scenario sets

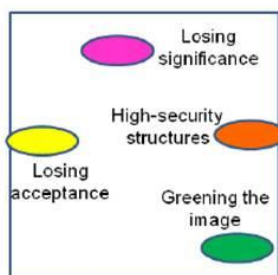
Scenario space



Cyber infrastructure



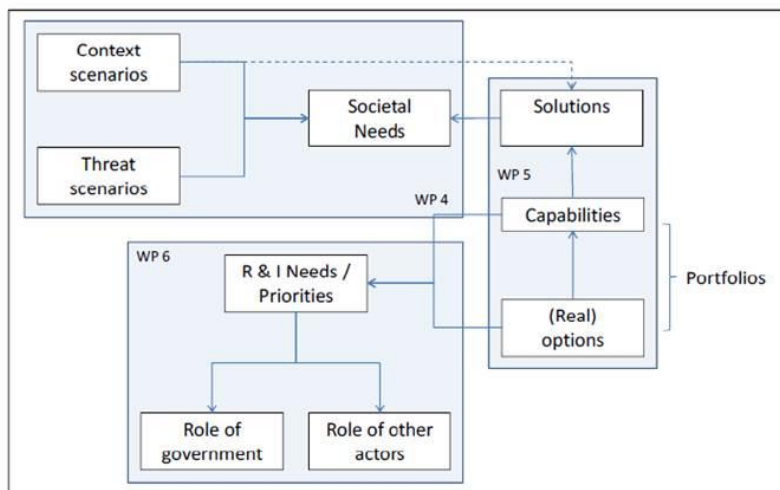
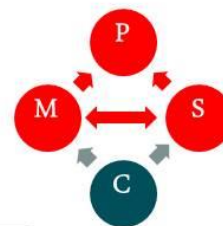
nuclear



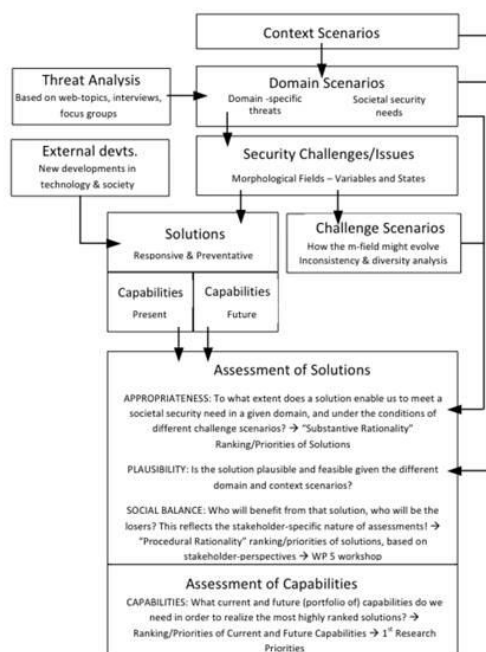
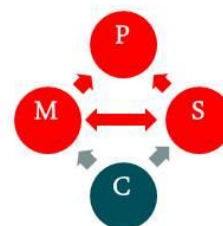
environment



The bigger picture...



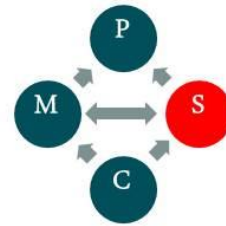
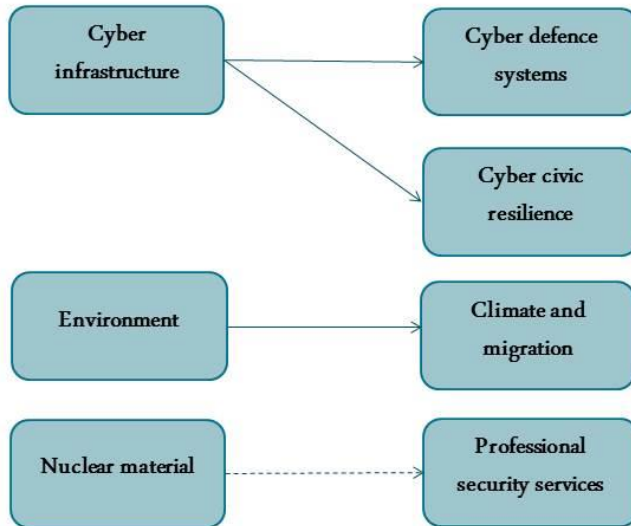
The bigger picture needs to get smaller...



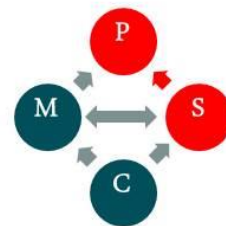
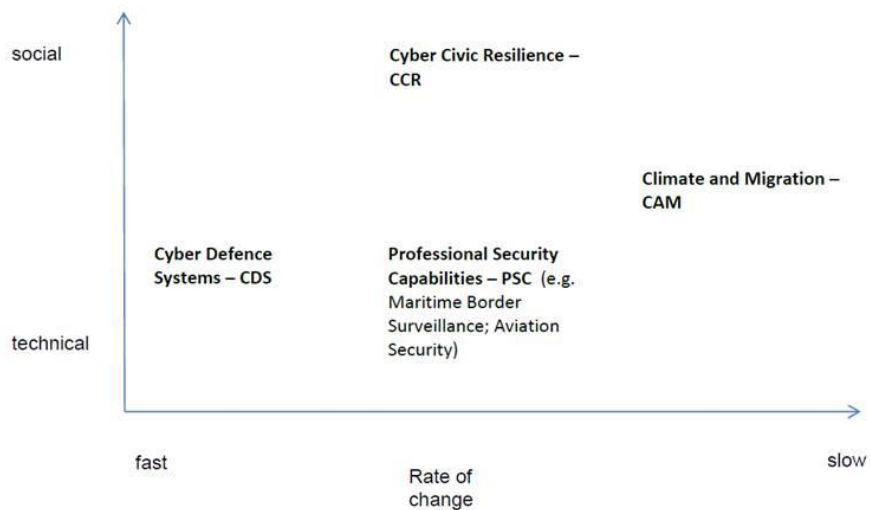
...comes the new PO...

Three domains

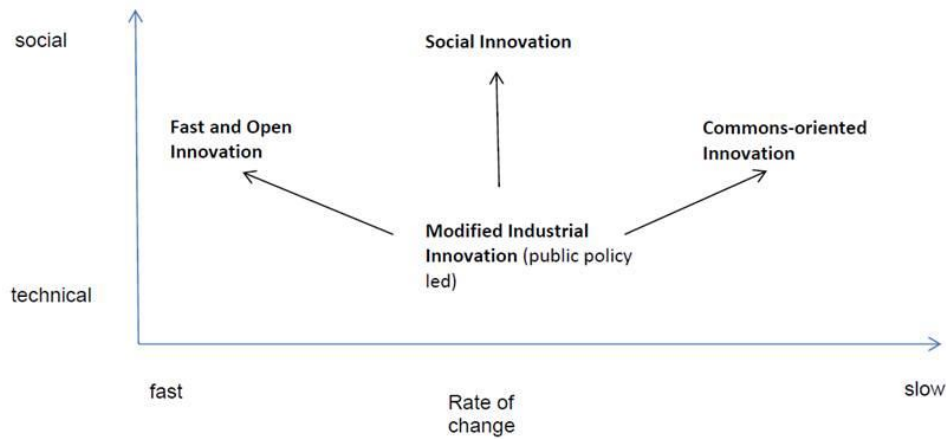
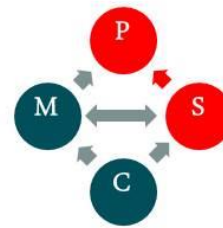
Four case studies



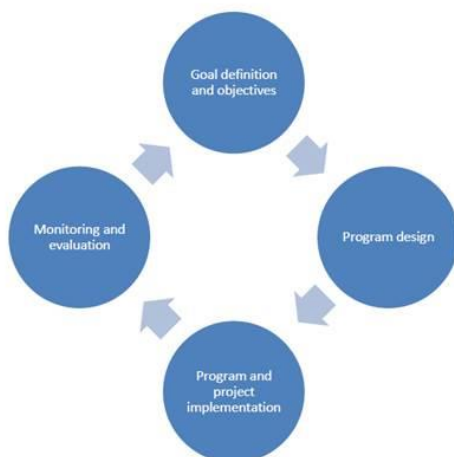
Positioning the cases



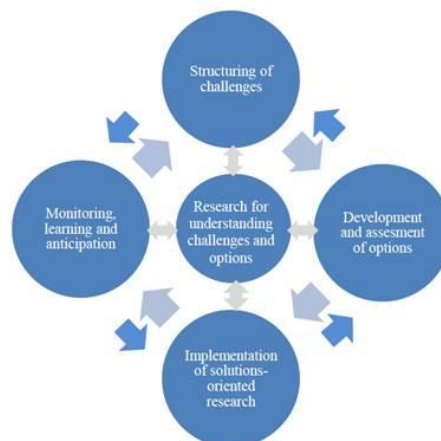
Four archetypes of security innovation



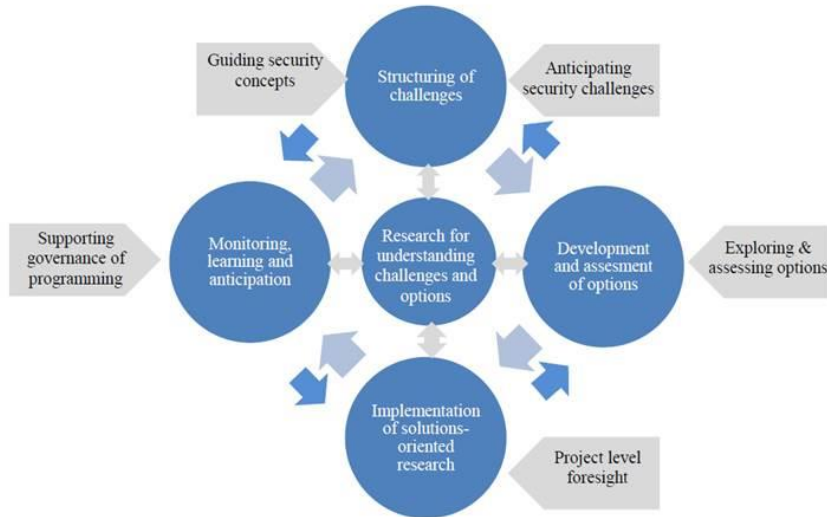
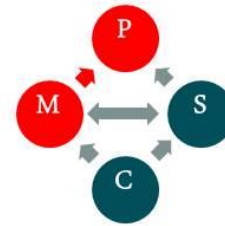
A standard four-phase model of R&I programming



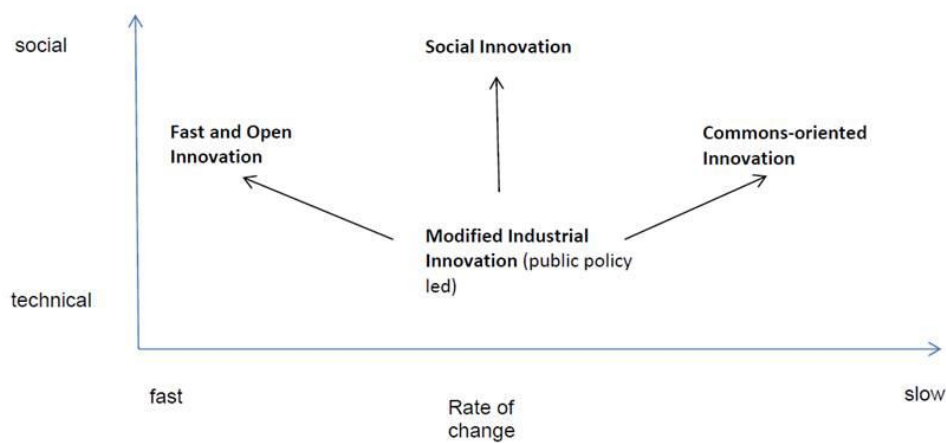
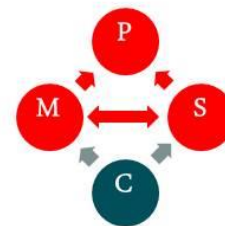
Adaptive four-phase model of programming for challenge-oriented R&I

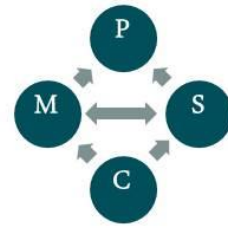


The roles of ETTIS foresight building blocks in the adapted programming cycle



Four archetypes of security innovation





Thank you for now!

eae@foi.se

6.3 LETTER OF MARIA DA GRACA CARVALHO

Ladies and gentlemen

Could I begin by thanking you the kind invitation to speak in such an important event. Unfortunately last minute engagements in my new function inside the EC prevent me of being with you. I am sending my speech.

The main purpose of my speech is to give you a brief overview of the most pertinent aspects to the H2020 programme. I shall begin with some general remarks concerning H2020 before going on to consider the most pertinent examples in more detail. In this respect, I should like to focus on three main aspects. These are widening of participation, synergies with other funds and finally, I shall devote a little more attention to the way in which H2020 answers to the expectations of long term societal security needs and challenges.

So, to begin with, let me make a few remarks of a general nature with regard to H2020. It is my belief that European policy should be designed in such a way that it recognises the difficulties that Europe is faced with and supplies a series of pragmatically conceived solutions. H2020 is a cornerstone of this policy. Under H2020, an increased level of investment will be evenly distributed between three fundamental pillars: “excellence in science”, “industrial leadership” and “societal challenges”.

However, Horizon 2020 is much more than a funding programme: it will be a fundamental instrument in structuring research and innovation in Europe over the years to come. In particular, it should be as simple as possible; effectively and adequately funded, include a comprehensive approach to the passage from research to market and be designed in such a way as to overcome fragmentation and to encourage collaboration across Europe and beyond.

The Most Pertinent Aspects to H2020

Turning now to the most pertinent aspects to the H2020 programme, let me begin with

- a) the widening of participation. Horizon 2020 places considerable emphasis on widening participation whilst

maintaining excellence as a main driver, on the one hand, and seeking to involve strong units of embryonic excellence such as small research groups and highly innovative start-ups, on the other hand.

Widening participation can be achieved by fostering greater transparency, through simplification of rules and the development of instruments such as return grants and twinning schemes. This will enable SMEs and smaller organisations to play a much more active role in the European research and innovation environment.

- b) My second point concerns synergies with other available funds. Achieving, at once, scientific excellence, and industrial competitiveness --- whilst meeting our societal challenges—is beyond the resources of a single programme. At the same time, Europe’s ambition to cover the whole cycle of innovation will inevitably require a multi-fund approach. For this reason, Horizon 2020 should be articulated with and complemented by other, parallel sources of European funding. In particular, European

“structural funds” could be deployed both upstream and downstream from Horizon 2020 to enhance capacity building and to facilitate the passage from concept to market.

- c) The final pertinent aspect that I should like to consider is that of a comprehensive approach to offer answers to the expectations of long term societal security needs and challenges.

The third pillar of H2020 addresses the most important societal challenge that Europe has to face in the near future. One of the societal challenges is devoted to ensure secure society as it was proposed by the European Parliament. The European Union, its citizens and its international partners are confronted with a range of security threats like crime, terrorism, and natural disasters, attacks against internet that may seriously affect essential sectors such as energy, transport, health and telecommunications. In order to anticipate, prevent and manage these threats, it is necessary to develop innovative technologies, solutions and to stimulate cooperation between providers and users to improve the competitiveness of European security, ICT and services industries.

With these objectives, the European Parliament has proposed a separate societal challenge on secure societies that includes topics such as:

- Fighting crime and terrorism
- Strengthening security through border management
- Providing cyber security
- Increasing Europe’s resilience to crises and disasters
- Ensuring privacy and freedom in the Internet

It was the conviction of the members of the European Parliament that support research on secure society, will contribute to the well-being of the European citizens.

Conclusion

To sum up in general terms: Horizon 2020 represents a rigorously conceived programme whose goal is to promote a flexible, inclusive and simple approach that will deploy diverse funding resources as effectively as possible. Aiming to support European industry, it also contains a concerted drive to promote excellence in science whilst meeting today’s societal challenges. Moreover H2020 aims to address the long-term societal security needs and challenges.

Thank you very much.

6.4 PRESENTATION OF NIKOS KASTRINOS



Foresight

**in the strategic programming of
Horizon 2020**

Nikos Kastrinos, Team Leader: Foresight
DG RTD A6: Science Policy, Foresight and Data

Presented at the ETTIS conference "Shaping Societal Security in the EU" , Brussels, 20/11/2014

* All views presented belong to the author and do not necessarily reflect the views of the European Commission



Contents

*Foresight and the EU (an ever changing
relationship)*

*Strategic Programming in R&I: the EFLA model
and H2020*

*Our experience with foresight and strategic
programming*



Foresight in the EU: the early phases

1974: Europe + 30

1978: FAST

1983 - 1987: FASTII (FP1)

1988 - 1991 MONITOR (FP2)

1989 FSU



Foresight in the EU: institutionalisation in R&I policy

1994-1998: FP4

- **IPTS**
- **ETAN**
- **Socio-economic Research**

1998 - 2014 (FP5, FP6, FP7)

- **Foresight research in the SSH programmes**

Research into FS, FS community development, and policy FS studies
Often in collaboration with GOPA/BEPA and JRC-IPTS

- **EFFLA in the Innovation Union (2011-2014)**

Emphasis on using foresight for R&I policy purposes

The current state of affairs: foresight in the EC

European Strategic Policy Centre (replacing BEPA)

- ESPAS

JRC

- Foresight and Behavioural Insights

CNECT

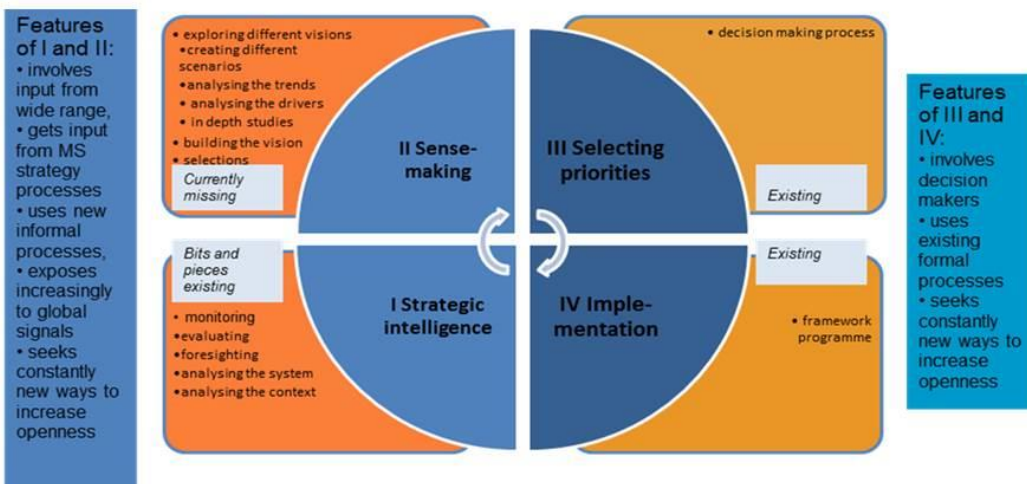
- Digital Futures / Futurium

R&I

- Foresight "main-streamed" (foresight projects and foresight in projects across the different parts of the programme)
- Foresight in Strategic Programming: coordination and "sense-making"



Foresight in strategic programming: the EFFLA model





Strategic Programming in H2020

Provides a coherent, evidence-based approach to implementing the activities set out in the Horizon 2020 Specific Programme

Supports an integrated approach, for areas that cut across different challenges and for linking key enabling technologies to societal challenges

Is not about reprioritising – but maximises impact of EU funding by ensuring that the programme responds to new developments,

Covers the full research and innovation cycle, and contributes significantly towards the EU's overall policy objectives



Extrapolating from the first Strategic programme of H2020

Possible cycles:

- **December 2014: 2nd Strategic Programme**
- **2014 - 2015: strategic intelligence for 3rd strategic Programme**
- **2015 – mid 2016: sense-making for 3rd Strategic Programme**
- **December 2016 Third Strategic Programme**
-



Inputs to the strategic programming process

Own intelligence:

- **Programme management**

Including foresight projects

- **Cross-cutting foresight**

Including policy related foresight

Stakeholder consultations

Expert Advice

Member States' input



Our activities and experience

September 2013 – March 2014: a pilot with foresight inputs:

- **A workshop with experts / a study**
- **A dedicated EFFLA policy brief**

Pilot "sense-making" projects (ongoing) on:

- **Key long term Transformations in R, I and HE**
- **Foresight and Trust**
- **Junction of Health, Environment and the Bioeconomy**

Aiming at contributing to the ideas underpinning strategic programme and work-programme texts





What have we learned?

All areas of H2020 are forward looking, but some are better than others at working with foresight

Absorption of foresight intelligence requires

- **a forward looking culture**
- **"anticipatory governance" structures**
- **discipline and good process planning**

in foresight: trusted intelligence source / messages are key

in strategy processes: calendars are key



*Thank you for your
attention!*



6.5 SPEECH OF TJIEN-KHOEN LIEM

- Many thanks for inviting me to this event. ETTIS is an important 'fore-sighting' project. As we all know, fore-sighting is difficult and it is a dangerous undertaking since it concerns 'things' what might happen in the future.
- Someone, a long time ago, told me: "beware, there are two types of 'foresighters': the ones that use the crystal ball and the ones that study the history books; I personally prefer the latter.
- Actually there is a third type: these are the ones that use EU research budget (and it is principally acceptable and is well justified to spend EU research budget for risky business).
- I have been with the European Commission for over 21 years now:
 - I came to join the Commission's services, DG Research (then DG XII) in April 1993 to help set-up the civil aeronautics research programme. Prior to that I worked for a large international corporation in the Aero Space and Defence business,
 - Shortly after '9/11' in 2001, I was among the people that prepared the EU Security Research,
 - Security Research, first under PASR (3 years, 2004, 2005 and 2006, 45 Mio €), then FP7 (2007 to 2013, 1,4 Billion €) and now H2020 (2014 – 2020, 1,6 Billion €),
 - The EU's Security Research was designed in DG Research, went to DG ENTR in 2005 and now under the Juncker Commission it is part of DG HOME, serving Mr. Dimitris Avramopoulos, the Greek Commissioner responsible for Migration, Home Affairs and Citizenship.
- When I came to Brussels in the spring of 1993, the 'Maastricht-Treaty' was new; it brought many changes, challenges but also new possibilities to the construction of 'Europe'. The main focus then, was still on shaping Europe in the aftermath of WW-2, particularly on the economic aspects thus, to providing and ensuring prosperity to the 'western' parts of the continent.
- What today became the European Union of 28 Member States; in 1993 it consisted of 12 Member States. Also, today we have a common currency for the 15 Euro countries. So, no doubt: the EU became very much wider and very much deeper too.
- but on the other hand: it is still struggling to shape the kind of security we want for our society,

- While working in this societal security field, it became clear to me that we must stop the 'reactive' way we tend to use, to want to provide 'security',
- Some examples: -We had terrorists cooking IEDs in their kitchens and we reacted by taking products containing high percentage acetones and hydrogen peroxide off the shop shelves. -We had someone trying to mix liquid explosives in an aircraft lavatory, then we ban liquids, and to make it even more expensive: we install very costly liquid scanners at airport security check points.
- Providing security to the society is a very complex matter; too complex for just wanting to solve the problem by providing 'patches' to insecurity breaches.
- There are almost infinite ways to breach security rules. We certainly do not want the burden of that many patches.
- On the long run we cannot afford to: 'just react'. We need a better understanding on the underlying issues. We also need to strengthen the resilience-ability of our society.
- Trends - in our society, and threats - to our society, are to be closely monitored. Mixed with the right understanding of our past and cultures, we should have the right formula to help define the right behaviour for the future. Structures are to be created, procedures developed and policies to be implemented
- Now, as I stand here today, we are 5 years into the 'Lisbon Treaty' and 15 years after the 'Amsterdam' treaty:
- The May 1999 - 'Treaty of Amsterdam', amends the Maastricht "Treaty on European Union". And the Amsterdam treaty meant a greater emphasis on **citizenship and the rights of individuals**, an attempt to achieve **more democracy** in the shape of increased powers for the European Parliament, the creation of **a Community area of freedom, security and justice**, and the beginnings of a **common foreign and security policy** (CFSP). The latter however is to remain closely in the hands of the Member States and in the foreign and security policy domains, the individual Member States will co-operate whenever they consider it necessary. The 'buzz-word' is "Second Pillar".
- Nevertheless it should be noted that:
 - citizenship,
 - the rights of individuals,
 - more democracy,
 - the creation of a Community area of freedom, security and justice,
 - and the beginnings of a common foreign and security policy,

...it all comes together in one package and that should denote our security culture.

- It is the 'Lisbon Treaty' however that is the great reformer. It gives us the means to better act together.
- The new 'Junker Commission' became operative on 1 Nov. 2014 and it is the first time the Commission is constituted under the Lisbon Treaty.
- Concerning 'External actions', President Junker stressed (quote) "We need better mechanisms in place to anticipate events early and to swiftly identify common responses. We need to be more effective in bringing together the tools of Europe's external action. Trade policy, development aid, our participation in international financial institutions and our neighbourhood policy must be combined and activated according to one and the same logic".
- The newly appointed High Representative for Foreign Affairs and Security Policy is Ms. Federica Mogherini. (by the way she has her offices in the Berlaymont building)
- She has a unique status under the Treaties, at once representing Member States as the Union's High Representative for Foreign and Security Policy and, at the same time, representing the Commission as one of its Vice-Presidents.
- In the Commission, the High Representative of the Union for Foreign Affairs and Security Policy/Vice-President will be responsible for the project of 'A Stronger Global Actor', helping to steer all of the Commission's external relations activities.
- In order to combine the tools available in the Commission in a more effective way, the High Representative will steer and coordinate the work, in particular, of the Commissioners for
 - European Neighbourhood Policy and Enlargement Negotiations (Hahn – AT),
 - Trade (Malmstrom – SE),
 - International Cooperation and Development (Mimica – CR),
 - Humanitarian Aid and Crisis Management (Stylianides – CY),and last but not least
 - Migration, Home Affairs and Citizenship (Avramopoulos – GR).
- The High Representative, as a Vice-President in the European Commission, must play her role fully within the College of Commissioners. To make this possible, whenever she sees the necessity to do so, she will ask the Commissioner for European Neighbourhood and Enlargement Negotiations (Hahn) and other Commissioners to deputise in areas related to Commission competence.

- So, the relevant Commission support structure for the HR is well defined and is in place,
- Nevertheless, a friend -policy analyst, of me, rightly said recently: that the HR's dual role is reflecting the wish of many EU countries to have “hard” foreign policy dealt with at intergovernmental level in the Council, while key soft power tools are in the Commission’s competence.

- Today's changing world calls for Europe to take on a greater role in ensuring international peace and security. Europe needs to ensure it has the capabilities at its disposal that meet the needs.
- In this context, the EU needs to strengthen the following objectives:
 - Operational effectiveness. It's about being able to better respond to crises and to deploy the right capabilities quickly and effectively.
 - Security and defence capabilities. It's about aligning military and civilian capabilities with the needs of the future. More systematic and longer term European cooperation could help to plug the capability gaps.
 - Developing a more integrated and competitive industrial bases for the European security and defence industries, for example through a well-functioning market and development.
 - Promoting relevant research that is able to respond to current and future needs.
- The EU foreign and security policy depends on the ability of the EU's Aero-Space, Defence and Security industry to provide the required equipment, meeting the EU's needs and ambitions. We need to strengthen the sector's technology basis.
- In its Conclusions in December 2013, the European Council said: "... welcomes the Commission's intention to evaluate how the results under Horizon 2020 could also benefit defence and security industrial capabilities”.
- It invites the Commission and the EDA to work closely with MSs to develop proposals to stimulate further dual-use research. A Preparatory Action on CSDP-related research will be set up, while seeking synergies with national research programmes whenever possible."
- On Research and Dual-use:
 - The increasingly dual character of technologies calls for a comprehensive approach in R&D.

- The Commission already works closely with the EDA to maximise synergies between civilian and defence research.
 - The Commission and the EDA have agreed to coordinate their research activities in specific topics (CBRN, cyber security) under the European Framework Cooperation. It was the first step for maximising complementarity among civilian security and defence-related security.
 - The European institutions are promoting dual use synergies taking into account: interface between civil and defence actors; synchronized capability planning; development of 'hybrid standards' (e.g. software defined radio and certain technological requirements for unmanned aircraft systems).
 - The research funding programme Horizon 2020 has a civilian focus, but already supports, to a limited extent, research related to CSDP, where there are common civil and CSDP needs.
 - The Secure Societies Challenge of Horizon 2020 includes a thematic priority, Border Security and External Security, aimed at supporting the Union's external policies, mainly civil-oriented security research.
 - We will now explore how the scope of this cooperation can be extended, possibly for example in the area of Key Enabling Technologies.
 - We are also exploring the best way for establishing the Preparatory Action on CSDP-related research as endorsed by the European Council. This would be outside of the framework of Horizon 2020; to run for maximum 3 years and will have a relatively small budget – likely to be a maximum €50 million. Thereby, to maximize the Civ-Mil synergies, taking into account the H2020 parts specifically "Secure Societies" but also other relevant parts of H2020.
 - While this proposal is, in itself limited, it is of strategic importance since, if successful, it could make the case for a possible inclusion of CSDP-related defence research into the next European Framework Programme for Research starting in 2021.
 - Any proposal for the scheme would have to be approved by both the Council and the European Parliament.
- So, to conclude, The "Secure Societies" part of H2020 has parts that are relevant to CSDP. For that matter, other areas of H2020 might be relevant to the need to support CSDP. However, any H2020 funded activities will maintain its principle 'Civilian' Focus .
 - The CSDP-PA and accordingly the possible future research programme resulting therefrom will be complementary.

- The debate is ongoing as what research the PA should support and particularly what the future large research programme should aim at.
- The answer –in my personal opinion, should be sought in the text of Art. 42 and 43 of the TEU.
- Quote: Art. 42 TEU: “The common security and defence policy shall be an integral part of the common foreign and security policy. It shall provide the Union with an operational capacity drawing on civilian and military assets. The Union may use them on missions outside the Union for peacekeeping, conflict prevention and strengthening international security in accordance with the principles of the United Nations Charter.”
- Quote: Art. 43 TEU: “1. The tasks referred to in Article 42 (1), in the course of which the Union may use civilian and military means, shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories”.
- I must also say that according to Art. 42 TEU, “safeguarding national security remains the sole responsibility of each Member State”. The Commission accordingly, when preparing legislation, must carefully scrutinise that the envisaged measures fall within the competence of the Union.
- There remains a lot to be done and that promise for more extensive Foresighting work and projects.
- Thank you very much for your attention.

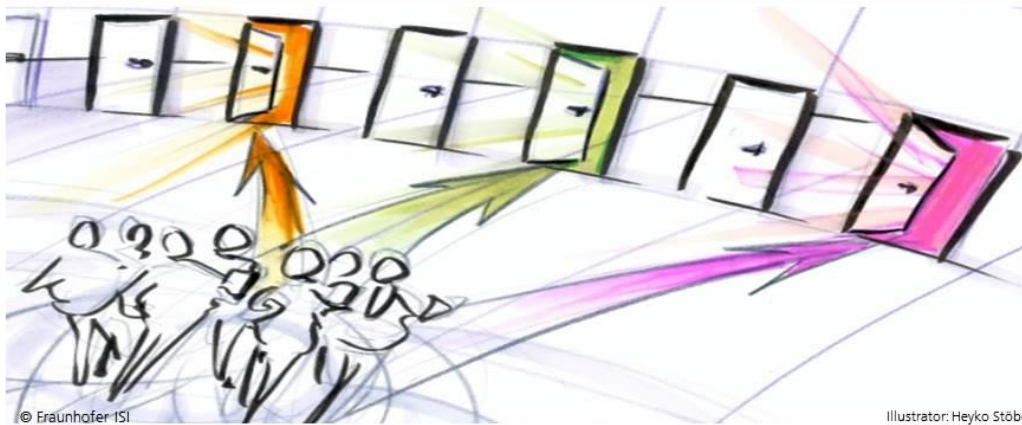
6.6 PRESENTATION OF ANTJE BIERWISCH

CIVIL SECURITY RESEARCH – FUTURE CHALLENGES AND METHODOLOGICAL OUTLOOK

Dr. Antje Bierwisch | Fraunhofer ISI | Competence Center Foresight

Shaping societal security in the European Union – A High Level Event

Brussels, 20th of November 2014



© Fraunhofer ISI

Fraunhofer
ISI

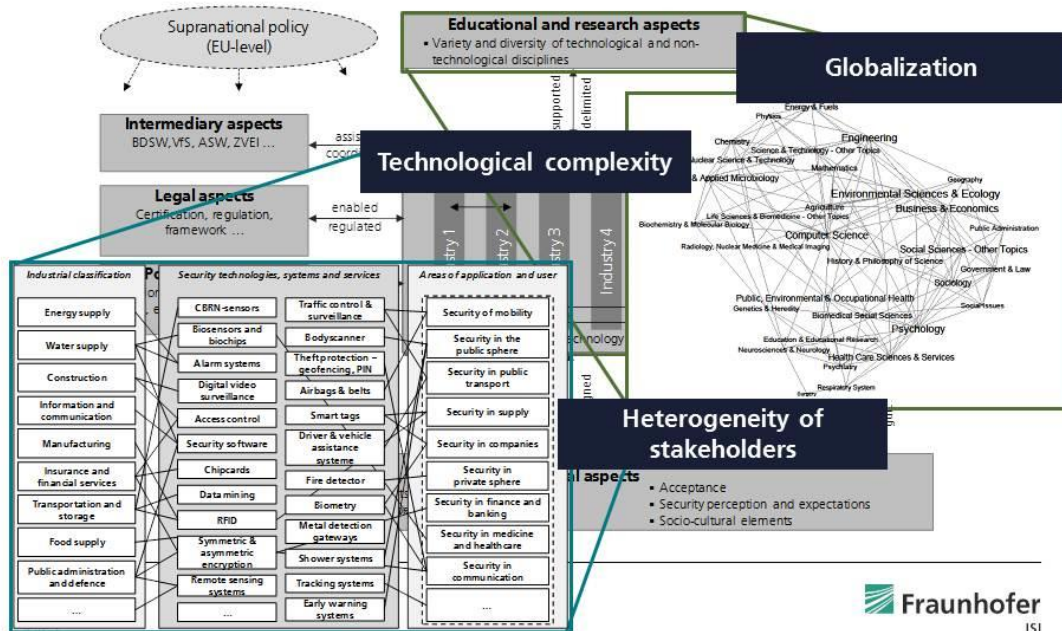
Outline



© Fraunhofer ISI
Seite 2

Fraunhofer
ISI

Civil security system of innovation Germany - Complexity of ...



Starting points: Challenges within the STI-Policy for civil security

- **security research and policy** - due to their strong penetration depth in **ethical, legal, societal and political** action patterns as well as the basic assumptions of societal cohesion (e.g. understanding of privacy, perception of security, attitude towards security)

Requires ...

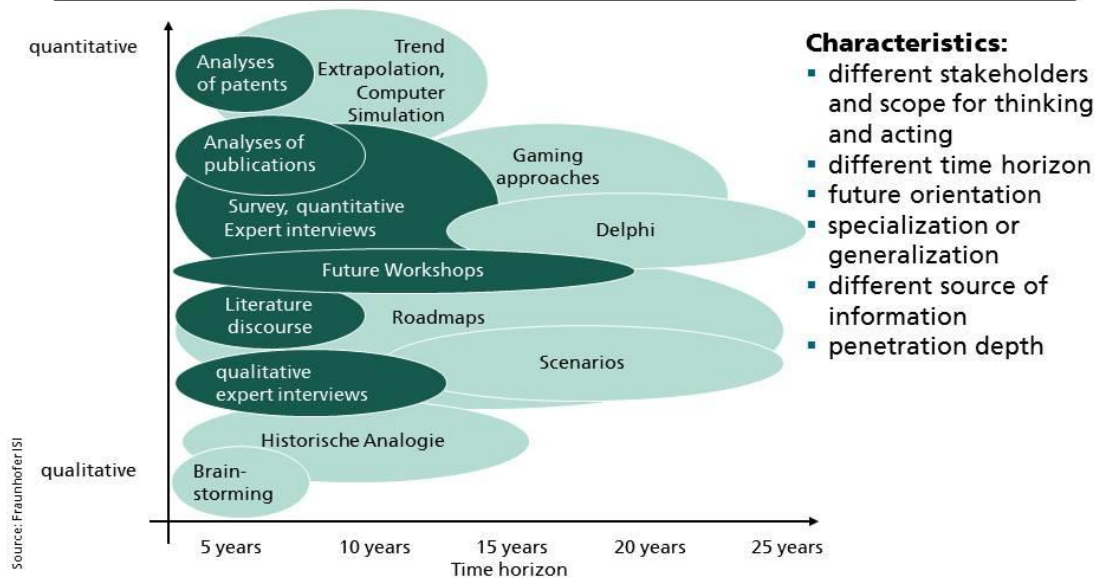
- **RRI – Responsible Research and Innovation** – basic requirements for the future European research landscape :

- **main purpose** for future science and research or the **necessary capability** for Europe to deal with societal challenges in the future
- Increasing requirements for the design of future research and innovation concepts:
 - support the **dialogue** between science and further sub-systems of society
 - most possible involvement of **stakeholders** in the R&D process
 - address the current and future **societal needs** and objectives of the society
 - reflection of underlying **values**, and
 - **sense of responsibility** in research, technology and innovation processes

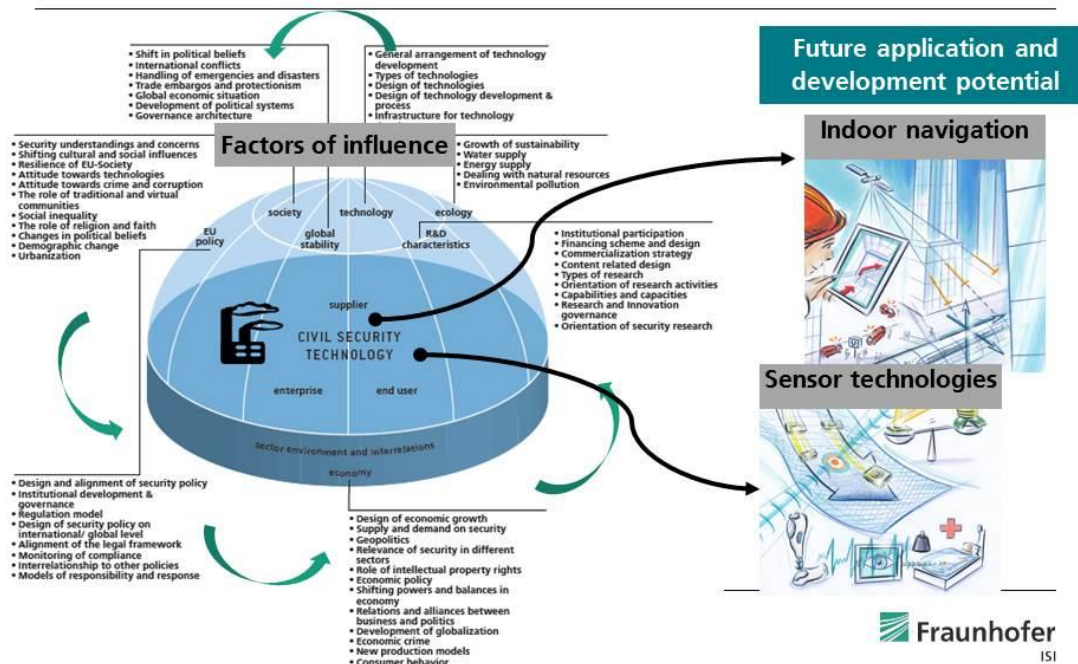
Outline



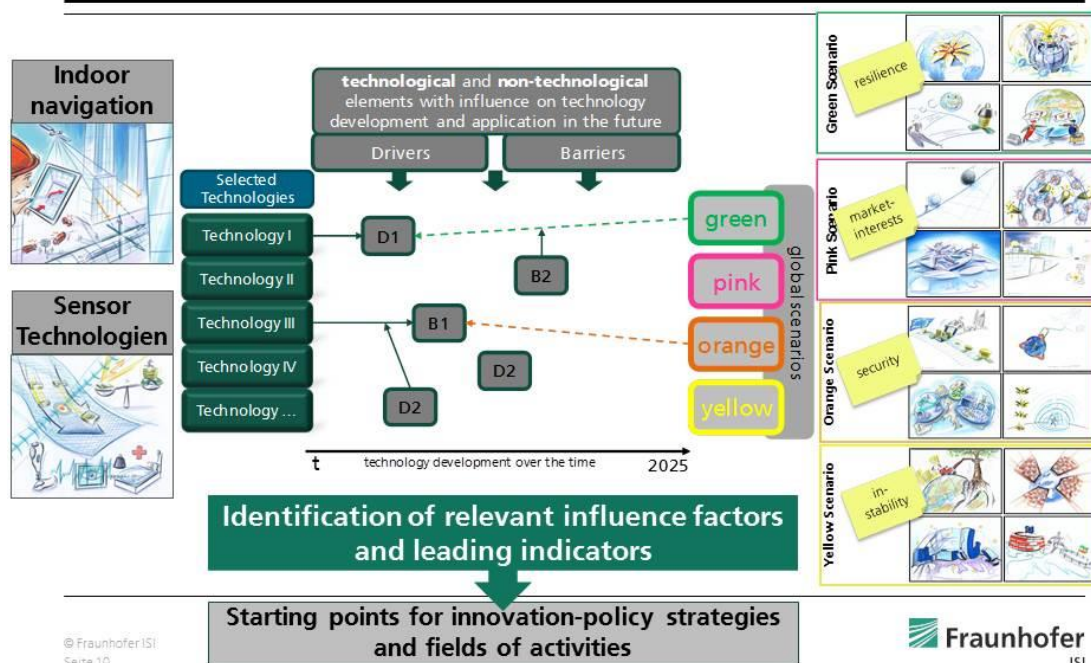
Identification and Anticipation of future trends and needs



Scenario based technology assesement: Emerging civil security technologies...ETCETERA

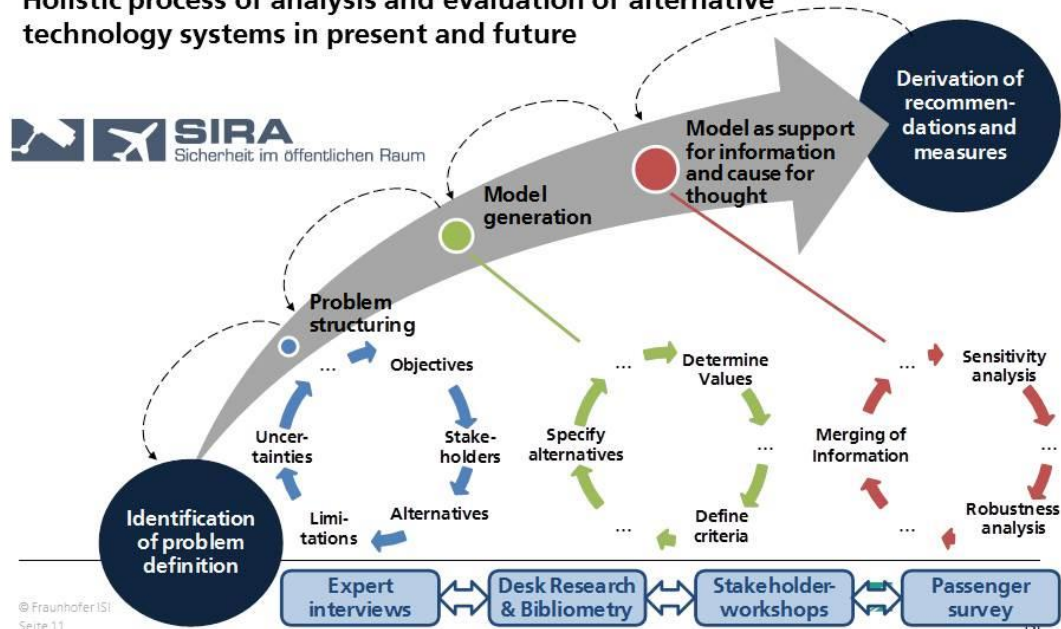


Scenario based technology evaluation of emerging civil security technologies...ETCETERA

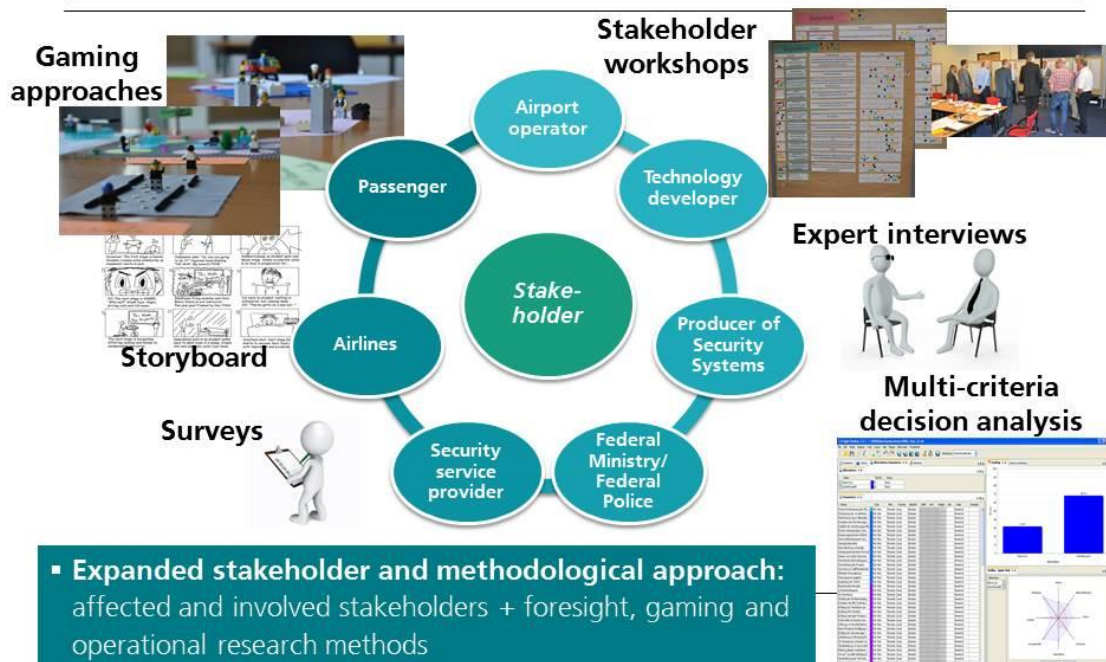


The future design of passenger controls at airport – security in public spaces

Holistic process of analysis and evaluation of alternative technology systems in present and future



Enlargement of stakeholder involvement and methodological approach



Outline



Points to discuss



- How do deal with cultural differences in perception and attitude towards security?
- How to increase awareness or acceptance of such participative research on the side of policy makers?
- Need for methodological guidelines or standards for such integrated research approaches (e.g. stakeholder involvement, RRI)
- Need for systematic monitoring integration of available or new data sources due to case related solutions – systematic integration of large scale database (technical, social, economical databases ...), e.g. KETs observatory
- Need for new indicators and methods, which kind of data and information are necessary - adaption of new methods

Thanks for your attention!



Contact details

Dr. Antje Bierwisch

Competence Center Foresight

Fraunhofer Institute for System and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany

Phone: +49 (0) 721 / 68 09 - 374
Fax: +49 (0) 721 / 68 09 - 330
Email: antje.bierwisch@isi.fraunhofer.de

For further information:

<http://www.sira-security.de/en>

<http://www.isi.fraunhofer.de/isi-de/v/projekte/SIRA.php>



6.7 SPEECH OF J. PETER BURGESS

From technological potential to societal planning:

The ETTIS approach to security foresighting

The impact of the future on the present

In 2007, the essayist, scholar and statistician, Nassim Nicholas Taleb published the influential book, *The Black Swan: The Impact of the Highly Improbable*. That book, which has become known as an expression of the ‘Black Swan’ theory, is a study in the character of future events.³

In *The Black Swan*, Taleb distinguishes between different kinds of future events. All future events take place, of course, in the future. But Taleb goes beyond this simple fact. He notes that there are important differences between kinds of futures, between different relationships of present to future, between what kind of possible paths can lead to different future outcomes. Most importantly, Taleb clarifies and nuances the different ways that the future can impact upon the present.

The future, according to Taleb, is not just ‘what happens’. It’s ordered and valorised according to what way it relates to the present, according to its likelihood, first and foremost, but also according to the way this likelihood plays out in our attitudes toward the future, our confidence or despair, our concerns, about what has not yet taken place, what is not yet even a fact. In Taleb’s understanding of futurology, knowledge of the future is gradated, not only according to likelihood or probability, but also in terms of impact upon the present.

He uses the figure of the ‘black swan’ as a way to reflect not only upon what we actually know or do not know about the future, but also about how we experience we know what we know or don’t know about the future, about what impact it has on our lives and on our vision of our future.

The relation between the known and the unknown, he shows, is not merely empirical. It’s not a flat, homogenous series of facts or events, a kind repetition or continuation of what is going on now. Rather, it is asymmetrical. The unknown, in addition to being empirically unknown, also has an effect. It has an aesthetic, moral, cultural, even the material effect just by virtue of it being unknown.

In other words, the asymmetry (or imbalance) of the known present and the unknown future lies not only in its factual difference, but in the force of astonishment or the shock of the future unexpectedly becoming reality, unexpectedly becoming known. There is a near *moral* reaction or indignation at it appearing in a way that did not—or maybe did—correspond to our preparations for dealing with the world, with our plans, our projects, our investments, our hopes and dreams.

This astonishment—or perhaps indifference—at the future becoming present makes a statement about us, about our knowledge of ourselves and our surroundings.

The ‘black swan’, is what Taleb calls an outlier, a phenomenon that lies ‘outside the realm of regular expectations’ something which cannot be immediately ordered into any given chain of events. Such outlier phenomena, he argues, are characterised by three qualities:

³ Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, London: Penguin Books, 2010.

- (1) First, ‘rarity’, that is, they lie outside of regular experience in the sense that nothing from the past adequately indicates that they should normally take place.
- (2) Second, they display ‘extreme impact’, in other words, they have effects which also lie outside of the ordinary.
- (3) And, third, they have ‘retrospective predictability’, In other words, despite the fact that they are both unexpected and have unexpected impact, we have an uncanny capacity for creating completely coherent and cogent explanations for them *after* they have happened.

Black swans have extraordinary impact on the world for two fundamental reasons, according to Taleb.

- (1) The first reason is entirely conventional: the force of the event itself. Obviously, the onset of World War I, the Crash of 1929, the oil crisis of 1972, the Chernobyl accident in 1989, the attacks of 9/11, etc. all had the real, empirical effects that are known and documented or which are in any case knowable.
- (2) But the second reason for the impact of the future on the present is stranger. It is related in a sense to the first. But it does not concern knowledge of events or facts. It concerns *non-knowledge*. It concerns what we do not know. Or rather it concerns what we know *now* but did not know before, before when such knowledge could have made a difference. It concerns the unpredictability of the phenomenon. The knowledge of *what* didn’t know, *that* we didn’t know and a moral insight about the meaning of this ignorance.

Clearly, this unpredictability is also empirical. It’s also a fact. The event that was simply and factually not foreseen is nonetheless a real empirical event. The innovation in Taleb’s discovery lies in the realisation that this secondary fact has immense historical force, immense impact on our understanding of the world. The secondary effect unites facts and human values: two domains of experience that none of the sciences, be they natural or social or human are equipped to entirely account for. This secondary effect manifests how facts themselves, through their experience, contain emotion, longing, hopes and aspirations, fears and disappointments.

Neither the natural sciences nor the human and societal sciences have really managed to get this point.

Rather, the sciences—the social sciences—in particular have dealt with this phenomena backwards. As Taleb points out, since the beginnings of risk and risk analysis, the social sciences have pretended to possess tools capable of measuring uncertainty as though it were an empirical phenomenon, something like measuring temperature. The insurance and finance industries have brought this illusion to the highest levels: the uncertainty of loss is adequately calculated in order to eliminate it from the equation of profit. Yet in a very real sense, what we do not know has far greater historical consequences than what we do know. What we do not know is what cannot conceivably happen. When it does happen, against all conceptualised likelihood, its meaning is immense.

Yet not only is the experience of the unknown a problem for the sciences because of the non-scientific moral values it puts into action. The knowledge itself is *based* on the values. We did not know these things would happen. And if we *had known* they would happen, then they would not have happened. The historical weight or meaning future threats is derived from their unpredictability, from the fact that we did not know.

As Taleb puts it:

had the risk [of 9/11] been reasonably *conceivable* on September 10, it would not have happened. If such a possibility were deemed worthy of attention, fighter planes would have circled the sky above the twin towers, airplanes would have had locked bullet-proof doors, and the attack would not have taken place, period. Something else might have taken place. What? I don't know (Taleb, 2007: xix).

What is uncanny here is that the non-knowledge is often more meaningful than the knowledge. What we *do not know* has greater impact than what we do know. Or, our non-knowledge produces consequences far greater than those that our knowledge would have produced.

The whole logical opposition between facts (which have meaning, consequences, etc.) and non-facts, fiction, poetry, images, etc., is in this sense problematic. What happens happens, not simply, autonomously, unproblematically as a singular event, without past or future. What happens, happens because it was not supposed to happen. The non-knowledge of the event is deeply imbedded in the causality of the event.

Thus, according to Taleb, the correct formula for harmless ignorance is not—as our mothers told us—‘what you do not know cannot hurt you.’ It is rather ‘what you *do* know cannot hurt you’. What you *do know* is exactly what can hurt you. For what we *do know* has already entered the empirical world, has already taken place. The damage is done, the lives are lost.

In a surprising formulation Taleb then asks ‘why does reading the newspaper actually *decrease* your knowledge of the world?’. Well it's because the major phenomena of life already belong to the past. They never will have been known in the present. They will never appear on the epistemological radar screen before passing into the past. They will never be really real, operationalisable knowledge about what is. The knowledge that really could change something in relation to what is happening is invisible to us in the moment of truth, in the moment of decision or responsibility. Knowledge that could make a difference is not recognisable as knowledge that could make a difference because we cannot know what it will ultimately make a difference about.

We cannot know that a plane flying off course implies a terrorist attack unless we *already* know it. Yet history has shown that the gatekeepers in our minds and hearts have an immense capacity to block out what is for us beyond the imaginable.

What can reading *The Black Swan* tell us about what we call ‘*security foresighting*’ today and about the assumptions and aims of the ETTIS project?

The challenge of ETTIS

The ETTIS project has had as its aim to identify future security threats so that we can prepare for them. At first glance, this task seems quite straight-forward. But it becomes quickly very complex. This complexity can be summed up in terms of 3 challenges:

The challenge of knowledge. The first, obvious challenge of foresighting is of course that it is about the future. The future hasn't happened yet. We don't know what happens in the future. Indeed the future is entirely unknown. Strictly speaking, *anything* can happen. But, fortunately, in more pragmatic terms, many things will probably *not* happen. While we cannot know with certainty what will happen, we can reduce the number of options.

The challenge of needs. The second challenge is that we don't know what we will need, what kinds of security we will be required in the future, what we will be under threat from, what dangers will be present, what risks we will face, etc. Certain things that create fear, anxiety, uncertainty today, may not have the same effect in the future. And by the same token, it's entirely possible that what we fear today will be completely different from what we have to fear tomorrow.

The challenge of capabilities. The third challenge is that we—that is, European society, representatives of society, citizens, authorities, etc.—will not be capable of doing just anything in the future. While it's true, that we don't know what we will be capable of, what capacities we will have, or what resources we will have, we probably won't be able to do what ever we want. We won't be able to fly over tall buildings like superman, or be two places at the same time, or breath without oxygen. There are limits to our options. So what we can actually do in the future, and what we can do in response to what happens in the future is probably limited.

To summarise: the three-fold challenge of ETTIS:

- (1) We don't know what will happen in the future, but we can eliminate some things;
- (2) We don't know what security *needs* we will have in the future;
- (3) We don't know what our capacities will be in the future, but we can eliminate some things; and

Most approaches to trying to plan for the future focus on the third challenge: capabilities. They try to understand what our future capabilities are, then to steer those capabilities so that we are best equipped to meet the first two challenges, namely that we do not know what will happen, nor what we will be threatened by.

Capability approaches are most commonly based on economic, technological or organisational categories: We want to prepare for future dangers by making sure that we have the equipment and expertise needed to face the dangers, and that we organise the work of security authorities in order to best. And we assume that well-planned security research will be able to reduce the gap between the known and the unknown, and increase the likelihood that we will be prepared.

If we get the facts wrong, then we are in trouble. If we through the force of our greatest foresighting minds come to the conclusion that the greatest challenge will be pandemic health crisis when in reality our greatest danger is a new generation of cyber intrusions, we will be a bad situation.

The most common approach to this kind of problem is that it is about getting the future facts right. The future is conceived and understood as a set of facts, as a set of claims about what the world is and what it is not, what the threats are and what they are not, what capabilities we have, which we do not. It will either be true (or not) that average life-expectancy for women in Iceland will be 85 years. It will either be true (or not) that the 16% of the African publication has access to internet, etc.

In the framework of fact-based approaches, we are dependent upon the facts about the future being correct, or close to correct. This dependency brings with it dangers of its own. The very fact that we are dependent on facts, on factual knowledge represents a risk, a security risk.

It requires that we develop a kind of risk assessment that not only assesses the danger of the threats, i.e. the danger of a pandemic crisis or cyber intrusion—events that would be dangerous enough—but also the insecurity of getting the facts wrong. Taleb's lesson to us is

this: not only is there uncertainty in about what will happen in the future, what dangers we will face, the uncertainty is itself a source of insecurity.

Thus the question: can we prepare for the dangers of the future in a non-fact-based way? How do we bridge the three gaps in our three challenges:

- (1) the gap between what we know about the present and what we don't know about the future;
- (2) the gap between our needs for security against threat now and in the future,
- (3) the gap between what are able to do at present and will be able to do in the future; and
- (4) the gap between the security that knowledge of the future gives us and the insecurity that uncertainty gives us?

Human futures

Security foresighting has typically sought to understand facts, needs and capabilities, in terms of industrial innovation, economics, organisations and technologies. This approach has left it chained to the pesky problem of facts, or rather to the lack of facts. When it comes to the future, facts are what we do not have.

The ETTIS project has sought to contribute an alternative to fact-dependent futurology, more oriented toward society, toward the human, toward the cultural dimensions that we believe contribute strongly to the security of societies.

Thus if we return to our three challenges. We can identify 3 gaps.

- (1) *The knowledge gap.* The gap between what we know about the present and what we don't know about the future, the missing facts, are part of a societal frame, a matrix of cultural traditions, norms, value expressions, that are woven together with strong continuity. For example: the continuity of mobile phone technologies lies not in the path connecting the constantly growing processor speed, but in the in path connecting how our everyday lives are shaped by increasing processor speed. These societal clues to the security puzzle have immense predictive power since they represent cohesion, continuity, interconnection, and coherence. While societal understanding tells us nothing new about facts. It tells us a lot about the values and identities that bind the past to the present and the future.
- (2) *The needs gap.* The gap between our needs for security against threat now and in the future is also deeply imbedded in the way that society evolves. It's linked to the way that people understand each other—and how these understandings evolve in time. It's linked to the way they live together, they way they eat and drink and worship, how they interrelate with other cultures, how they spend their money, how much money they have, where they get, what technologies they interact. It has to do with who people think they are, their political views, their entitlements, what they think they have to gain and what they fear they have to lose.
- (3) *The capability gap.* The gap between what we are able to do at present and what we will be able to do in the future depends far more on the evolution of technology, of how we relate to things, to media, to devices, to a range of technologies and technological devices. But from the ETTIS perspective, the evolution of technologies can only be predicted on the assumption that technologies evolve in and through social relations.

What can the ETTIS societal approach contribute with?

The ETTIS project has led to a range of ideas about how to do things differently, how to think about the future differently, how to plan public policy differently, and how to make investment strategy differently.

Here are 10 quick ideas that flow from the ETTIS output⁴:

- 1) Security research and innovation programmes should be guided by a broad understanding of society and its security needs. Research and innovation should start with analysis of society, analysis of how people live, work, play, travel, consume, love, fight, etc.
2. Security research and innovation should target a far broader range of people and interests. It should ask: who will be impacted by research and innovation, both positively and negatively? Who will benefit and how? For whom will it be detrimental and why?
3. The notion of security research and innovation should be opened up to account not only for technological innovation but for social innovation. How will be societies function in the future. In what ways will they generate their own security and in what ways will they interact with other security measures.
4. Security planning and innovation should have the possibility to adapt to not only technological change, but to social change. The life-cycle of a technology passes through many technical phases. But it also passes through different phases of social insertion, impact, acceptability by the public sphere, impact, etc.
5. Research and innovation should be contextual and adaptable to end-user needs as well. This is nothing new. However, flexibility in the concept of end-user is also needed. How does the end-use of security research evolve in time and in society. How is knowledge used, and how does research and knowledge production evolve based on such use.
6. Political processes need to be accounted for in security and research innovation. The interface with policy is not only crucial with regards the potential uptake and adjustment of innovations. It is crucial so that security measures are politically accountable, so that the public can have a voice in determining what can be done in their name, or in the name of their security.
7. Security research and innovation needs to be both inter-disciplinary and trans-disciplinary. Engineers alone cannot understand the security of society and how to achieve it, just like sociologists cannot understand software the fine points of software development. Good security solutions cannot be made in a vacuum or determined by a technology-steered market. (Where did we get the idea that it could?)
8. Security research needs to think locally and find local solutions. Security is dependent on society, on societal uptake, on expectation and needs. All these dimensions vary immensely from place to place, region to region, country to country.
9. Security research and innovation needs to think globally. Many security challenges that face society today are of a global character: environmental issues, pollution, pandemic, food security. A security research can only be successful if it accounts for the global dimension.
10. Security research and innovation should incorporate reflexion on the ethical issues it itself generates. Security is intimate. Security measures are in many cases intrusive. Societies

⁴ Freely after E. Anders Eriksson & Matthias Weber, How to foster security R&I able to support comprehensive societal security, ETTIS Policy Brief. <http://ettis-project.eu/wp-content/uploads/ETTIS-Policy-Brief-2-final2.pdf>

increasingly require that new developments in security measures carry with them new developments in ethical awareness.

Conclusion

Designing programmes of research and innovation means simultaneously letting go of what we cannot hold on to, and holding tightly to a future that is not yet even ours, a future that belongs to forces of innovation, social evolution, and human development, combined and orchestrated in a way no foresight can foresee.

The measures proposed by the ETTIS project therefore are partial, incomplete, *ad hoc*. They are anchored in our present, a present which—if we understand it correctly—will help us to understand the future and, strangely, paradoxically, uncomfortably, impairs us, handicaps us, even block us from the future.

On the other hand, if we understood everything the future has to offer, what security concerns and security needs and policy options the future will bring, then the future will also cease to have meaning for us. It will be a simple, homogeneous extension of the present.

6.8 PRESENTATION OF IDA HAISMA

The Hague Security Delta



HSD Corporate presentation

Ida Haisma – Director HSD

ETTIS Project
20 november 2014

www.thehaguesecuritydelta.com
[@HSD_NL](https://twitter.com/HSD_NL)



Europe's largest security cluster

Gateway to Europe and connected with the North American market

- Dutch security cluster with its core in The Hague, including:
 - Businesses, Knowledge institutions, Ministry of Security & Justice
 - Flagship initiative Dutch top sector High Tech Systems & Materials
- Strong ties with other (international) security regions & European Institutions
- Aim to enhance security & stimulate economic growth



12



Enhance security & stimulate economic development

Facts & Figures of Security Industry in The Netherlands (2012)

Businesses	<ul style="list-style-type: none"> 3,100 security companies (400 in region of The Hague) The Hague in particular strong in non-traditional, innovative security jobs & revenue
Revenue (€)	<ul style="list-style-type: none"> 6 billion euros (1,7 billion euros in region of The Hague) 4.1% yearly growth (2006-2010) despite economic downturn 50% growth expected by 2020 Forensics and cyber security main areas of growth
Jobs	<ul style="list-style-type: none"> 61,500 jobs (13,400 in region of The Hague) 25% job-growth expected by 2020



New risks demand new answers

Business, government and academic world need to tackle complexity together

- Supply and demand more closely aligned
- Use of technology driven security solutions
- Enhance radical innovation
- Economies of scale → aligned innovation budgets
- Availability of skilled and qualified personnel and graduates





5



Integrated Approach to Security

- National Innovation Agenda Security
- National investment agenda and 'Program Innovation Procurement Urgent' national government
- Cooperation between security partners: connecting local, regional, national, and European



6



Request Dutch Ministry of Security and Justice

“develop an National Innovation Agenda for Security, based on available material and knowledge, originated from:

- Needs and demands from public and private actors with a vested interest and position in maintaining, enforcing and enhancing societal/public security;
- Suppliers of technological, innovative developments, trends, developments, products services;
- “wildcards, serendipity”.

In order to constitute a “roadmap” consisting of national priorities for the innovation of the public security in the Netherlands.

HSD
The Hague Security Delta

7



Purpose

Bringing together demand, supply and knowledge to create societal/social and economic value

HSD
The Hague Security Delta



Function (1)

- Collective agenda
 - For public and private actors towards innovation in the field of security in the Netherlands;
 - To stimulate, arrange and manage a mindset for and a view on collective innovation ("together", co-working)
- Tuning of innovation needs and innovation supply
 - In order to select priorities for public partners including knowledge institutes ("triple-helix");
 - Create a individual and collective leverage, to realize "societal/social" (public) and "economic value" (private)



Function (2)

- Coupling of innovation processes and (innovative) procurement-, tender-, contracting processes
 - In order to create predictability in a solid, robust market for innovators, private actors, and (public and private) customers/demand organisations;
- Adopting the innovation theme's ("chapters") and javelins ("spearpoints");
 - By "coalitions of willing and able" (ownership)
 - Consortia (e.g. with regard to Horizon 2020/secure societies).

In order to create true economic value





The making of (1)	
January 2014	Take off by ministry of Security and Justice and HSD
February-August	Development of a "primary edition/longlist" and a variety of concepts based on multiple interviews (50 plus) and desk research
September	Version 0.9: consecutive approval in Executive Committee HSD, Advisory Council HSD, Board HSD
Oktober	Enhancing, completing the agenda, producing the agenda <ul style="list-style-type: none"> • Book/report (dutch) • Book/report (English in on-line format) • Website (tbd)





The making of (2)

November	Ratification/confirmation by secretary-general Ministry Security and Justice, secretary-general Ministry of Defense, director-general Ministry of Economic Affairs, Chairman of the Board Dutch National Police, Chairman Safety Council, Chairman Dutch Institute Physical Security, Chairman Technical University of Eindhoven, Chairman Tilburg University, Chairman of Delft Technical University, Chairman of Twente University, Dean of Leiden University, campus The Hague
2015	Development of the Innovation Agenda 2016

Measuring the effects and revenues of the 2015 version



Content; chapters (1)

- Comprehensive security; integrated data, networks and (eco-) systems, capabilities
- Innovation with regard to social and societal security; whole of society, security by design, societal and civic resilience
- Critical infrastructure (resilience, cybersecurity “internet of things”, integration, interdependencies)



14



Content; chapters (2)

- Netcentric working, information dissemination/validation/life-cycle in networked environments (social media, web 2.0, 3.0, social network analysis, interoperability, identity warranty, authentication)
- Surveillance and unmanned systems (concept development UAV-operations, civil-military cooperation, sensing, operational autonomy UAV operation)
- Proces innovation within and between professional organisations (operational decision making vs. norms and regulation for street-level bureaucrats, human factors, performance enhancing teams, serious gaming, functioning of heterogeneous teams)



15

Criteria for “admission” innovations in the agenda

- Innovation addresses vital/essential shortcoming or need (social/societal value)
- Must be widely usable on “systemlevel” (demands technical, social, processual combination)
- Requires collective approach, development (customers, innovators, suppliers, funders)
- Result is significant, substantial “turn over/trade volume”
- There's commitment and support in a “coalition of the willing and the able”
- Result in implementation in a period of 3-5 years (“looking towards 10 years”)





Dutch police is a resident at HSD, why?

Mark Wiebes, Chief of Police and Innovationmanager National Police

- National police is contractor for innovative security solutions
- Innovation is of key importance as an integral part of the police's work
- Close and intensive contacts between science, market, government and operational policework are required
- It's important to meet in informal ways, especially at the stage the ideas are formed
- HSD-campus is perfectly adapted to that end and helps "cross-over" understanding
- The National Police is easily accessible and approachable for innovation partners




Building track record

- 2012**
 - Start of The Hague Security Delta
- 2013**
 - Start of HSD Development Fund -*co-financing innovation*
 - The Hague Security Delta Foundation established
 - NFI contracted to build CSI Capetown (forensic innovation)
 - European Cyber Crime Center established in The Hague
 - Dutch Cyber Security Center established in The Hague
- 2014**
 - HSD Campus - *national innovation center for security*
 - Cyber Security Academy established in The Hague
 - World Nuclear Security Summit in The Hague
 - ASIS Europe 2014 conference in The Hague
 - Start of 8+ security innovation programs & projects
- 2015**
 - NATO to establish all ICT & cyber services in The Hague
 - 4th International Conference on Cyberspace in NL



6.9 PRESENTATION OF IAN BROWN

Global Centre for
Cyber Security Capacity-Building



- Our aim is to understand **how to deliver effective cyber security** both within the UK and internationally. We will make this knowledge available to governments, communities and organisations to **underpin the increase of their capacity** in ways appropriate to ensuring a cyber space which can continue to grow and innovate in support of well-being, human rights and prosperity for all



Foreign & Commonwealth
Office





Global
Cyber Security
Capacity Centre



- Collect case studies, examples of best practice
- Develop metrics and models of cyber security capacity maturity
- Disseminate and use metrics to drive improved practice





Dimensions of Capacity Maturity

Five complementary dimensions of capacity:

1. devising national cyber policy and cyber defence
2. encouraging responsible cyber culture within society
3. building cyber skills into the workforce and leadership
4. creating effective legal and regulatory frameworks
5. controlling risks through technology and processes

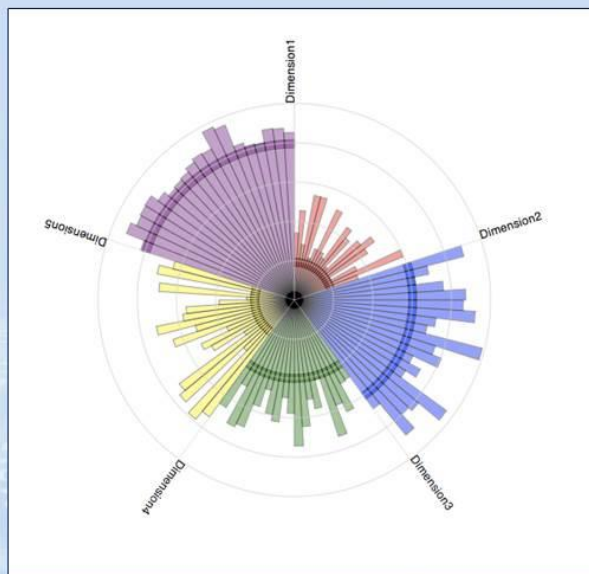


Work Thus Far

- Determining what existing research is being promoted in the international community
 - Avoid replication of efforts, as well as increase multi-stakeholder approaches to cyber capacity building.
- Cyber Capacity Factors - Draft for Consultation
 - Assessment of what factors are important in increasing cyber capacity across the five dimensions of the Centre, using expert panels of stakeholders for each dimension.
- Portal
 - In collaboration with the FCO and Said Business School, not only propagate the work of the Centre, but also to serve as a platform for the interchange of ideas on capacity building around the world.



- **Pruning:** is this factor already accounted for?
- **Categorising:** is this a factor, or evidence for the next level of maturity in that factor?
- **Feasibility:** can you practically measure the factor?
- **Validated:** how scientifically robust?
- **Potential:** if data is lacking, could it potentially be acquired?
- **Applicability:** are there bad or erroneous factors?
- **Effects:** Would you derive different conclusions based on your perspective of the effects?

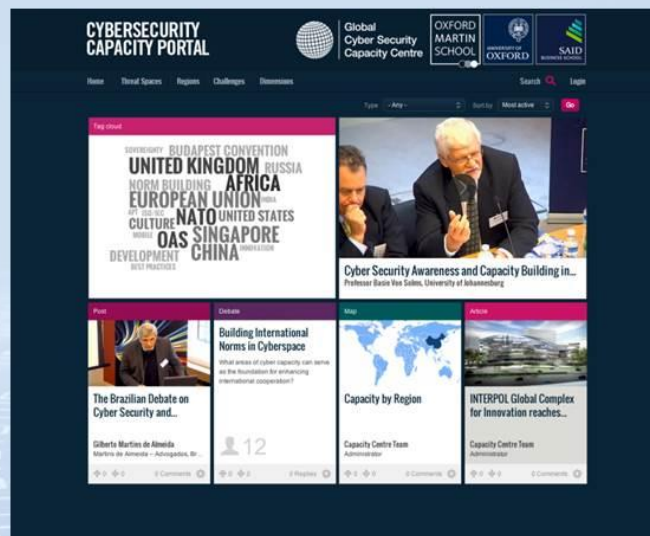


Multiple metrics for measuring maturity in each of the 5 dimensions

5 levels of maturity, solid bands indicating minimum level across all metrics for any particular dimension



- Start-up: At this level either nothing exists, or it is very embryonic in nature. It also includes "We've thought/talked about it - but haven't done anything" and "we observed no evidence"
- Formative: Some features of the sub-factor have begun to grow and be formulated, but may be haphazard, disorganized, poorly defined - or simply "new"
- Established: The elements of the sub-factor are in place, and working. There is not, however, well-thought out consideration of the relative allocation of resources
- Strategic (does not mean *important*: it is about choice). Choices have been made about which parts of the sub-factor are important, and which are less important for the particular organization/nation, contingent on particular circumstances
- Dynamic: there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat environment, global conflict, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies on the fly, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level



<http://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home>

new model of PhD/DPhil

- Promoted and funded by research councils
- £3.6m grant
- 12 funded places per year
 - UK / EU students
- Plus 5 places for self-funded (other sponsors, etc.) students
- Three annual intakes (initially)
- Research projects will be undertaken in a wide variety of academic Departments and disciplines
- Second similar centre separately funded at *Royal Holloway University of London*

usually
Master's
degree

year one:

- intensive education in cyber security
- two mini-projects (internships encouraged)
- seminars, industry 'deep dives', field trips

year two:

- *some taught courses*
- lots of reading
- develop a research plan

year three

- undertake research
- write papers

year four

- continue research
- write and submit thesis

First-year courses



Research Themes



6.10 PRESENTATION OF MATTHIAS WEBER



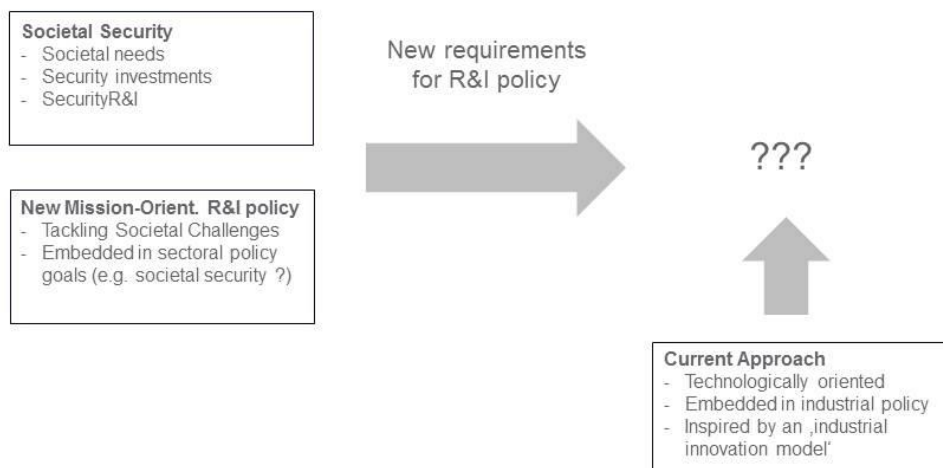
Mission-oriented RTI policy & programmes

The case of security

Matthias Weber

„Shaping Societal Security in the European Union“
ETTIS High-Level Event
Brussels, 20 November 2014

Why a new approach to security RTI policy and programming is needed



Implications for security R&I

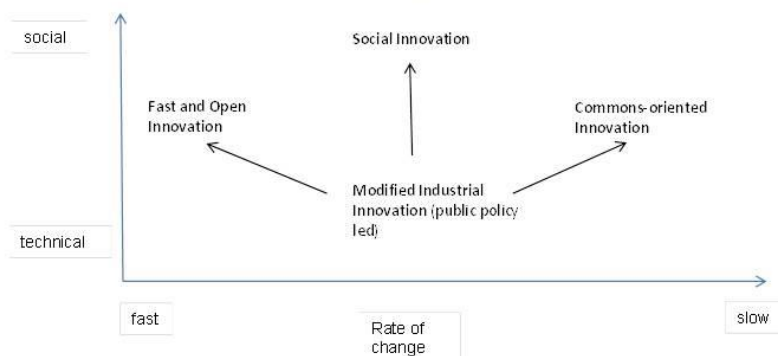
- Inherently limited incentives for innovation due to
 - Broad range of low-probability events
 - Public good character of security
 - New inroads for addressing security issues by way of R&I
 - Moving beyond threat-response model
 - More comprehensive set of targets of innovation: threats to as well as sources of security in the focus
 - Broader range of innovations to be considered: technological, social, organisational, etc.
 - Short as well as long time horizons
- ➔ A more differentiated approach to innovation (and R&I policy!) is needed!

21.11.2014

3

Four archetypes of security innovation

- Broadening of the range of innovation activities to be considered
- Two key dimensions
 - Rate of change – fast/slow
 - Balance between social and technological aspects



- ➔ Each innovation model raises different structural, institutional requirements, and thus also for R&I policy and programming

21.11.2014

4

The cases

- Professional Security Capabilities – mainstream ,modified industrial innovation model‘
 - Supply chain security and customs risk-based approaches
 - Geo-engineering
- Cyber Defence Systems – ,fast and open innovation model‘
- Cyber Civic Resilience – strong ,social innovation‘ elements
- Climate and Migration – ,commons-oriented innovation model‘

21.11.2014

5

Towards an adaptive programming cycle model

- From a linear to an interactive and adaptive programming cycle
- Deductive approach (vision – SRA – implementation) inappropriate
- Continuous adjustment of what constitutes the challenges and options
- Need for continuous „research for understanding“, underpinning all phases
- Flexibility in implementation: centralised vs. decentralised
- More actors and stakeholders involved, participatory approach, and in all phases
- Embedding in security policy – policy coordination



21.11.2014

6

Ten requirements for challenge-oriented security R&I programming

- Give guidance and orientation.
- Include the needs of those affected.
- Consider both social and technological innovation.
- Ensure flexibility and adaptivity
- Ensure embedding of R&I in the context of use
- Policy coordination
- Inter- and trans-disciplinarity
- Ensure specificity of local solutions
- Address a global geographic area of concern
- Consider ethical implications and dilemmas

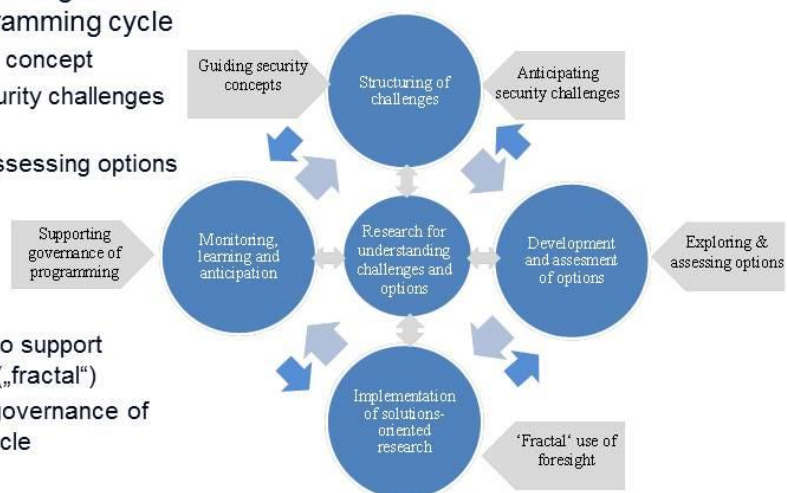
21.11.2014

7

The role of foresight in the adaptive programming cycle

- ETTIS foresight building blocks to underpin the programming cycle

- Guiding security concept
- Anticipating security challenges using scenarios
- Exploring and assessing options



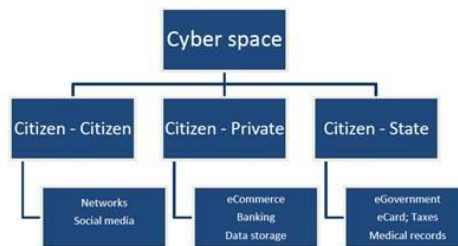
- Using foresight to support implementation („fractal“)
- Supporting the governance of programming cycle

21.11.2014

8

Example: the case of Cyber Civic Resilience CCR

- „Cyber“
 - Computers, computer networks and services
- „Civic“
 - Citizens perspective
- „Resilience“
 - Strength/ability of something to return to its original or better state after a disruption

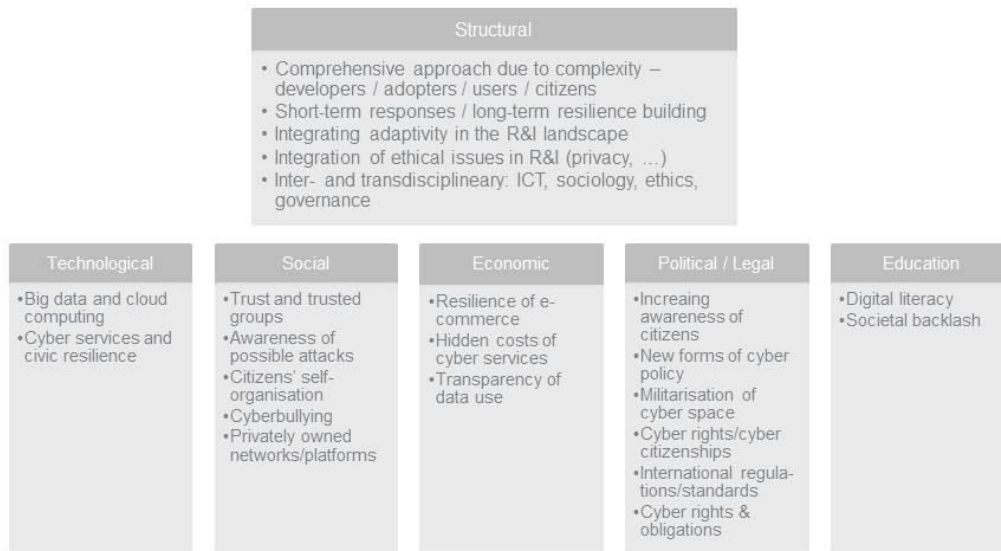


The identification of ‚Cyber Civic Resilience‘ is an example of a novel kind of R&I areas of different ‚shape and content‘

21.11.2014

9

Structural and thematic R&I agendas in CCR



21.11.2014

10

Concluding suggestions

- ‚Comprehensive societal security‘ as guiding normative concept for security R&I
 - Need for an security R&I strategy that provides normative guidance
- More differentiated approach to innovation (models) to underpin R&I policy
 - Abandon the prevailing „industrially inspired“ model
 - Take specific features of security seriously: ‚societal‘ nature of security, diversity, time/pace of change, adaptivity...
- Explore new approaches to programming
 - Adaptive and iterative approach
 - Decentralised vs. centralised
 - Integrating foresight
 - Research for understanding security challenges and solutions-oriented research

21.11.2014

11

Contact

Dr. Matthias Weber
AIT Austrian Institute of Technology
Innovation Systems Department
Vienna
matthias.weber@ait.ac.at

21.11.2014

12

6.11 SPEECH OF MONICA LAGACIO



Synthesis and Closing

Monica Lagazio
Three years of ETTIS
ETTIS High-Level Event
Brussels, 20 November 2014

ETTIS project started with the objective to address key problem areas in security

ETTIS Security Context

In an era of globalisation, growing interdependence and uncertainty security has gone through a significant transformation

-
- **What is the meaning of security and what needs to be secured ?**
 - Security has lost its national focus, while individuals and communities are becoming as important as states (i.e., societal security)
 - What is the meaning of societal security?
 - **How can we prioritise in a complex security landscape?**
 - Security has expanded to include several and diverse threats that are global in nature, have trans-national roots and are interconnected
 - Faced with limited resources and a much more complex security landscape how decision makers and end-user s can prioritise security spending and research efforts ?
 - **How can Europe support a fully integrated approach to security ?**
 - Given the new landscape, security needs a comprehensive approach cutting across national boundaries, sectors and departmental lines
 - How can multiple and different security stakeholder collaborate ?

ETTIS has produced several practical findings addressing the initial problem framework from several angles

- ***From traditional security to societal security:*** ETTIS has put forward an operational concept of societal security to support decision makers and end-users in practical settings
- ***Expanding the concept of 'innovation' as it pertains to societal research:*** ETTIS has developed a taxonomy of R&I models, better suited to cover the broader boundaries of societal security, which are based on the rate of change and the type of concerns at stake
- ***Practical processes for the identification of threats, needs, and solutions for society :*** ETTIS has developed tools, methodology and processes to assist researchers and policy makers identify threat, needs, and solutions within the societal security domain. This includes a three-step-process for the development of context-based threat scenarios and subsequent identification of threats and societal security needs
- ***Policy and priorities settings in societal security:*** ETTIS has made a contribution on how to identify research priorities and set up research agenda for societal security by putting forward an adaptive 4 phase model of planning

3

What's next for ETTIS?

....communicate ETTIS research results and support their uptake through



4

Contact

Dr. Monica Lagazio
Triateral Research & Consulting
London
monica.lagazio@trilateralresearch.com

25.11.2014

5